Measures of Resilience to Cyber Contagion – An Axiomatic Approach for Complex Systems

Gregor Svindland[a] and Alexander Voß[a]

[a]Institute of Actuarial and Financial Mathematics & House of Insurance, Leibniz University Hannover, Germany

February 5, 2024

We introduce a novel class of risk measures designed for the management of systemic risk in networks. In contrast to prevailing approaches, these risk measures target the *topological configuration* of the network in order to mitigate the propagation risk of contagious threats. While our discussion primarily revolves around the management of systemic cyber risks in digital networks, we concurrently draw parallels to risk management of other complex systems where analogous approaches may be adequate.

Keywords: Cyber Risk, Systemic Cyber Risk, Cyber Resilience, Cybersecurity, Systemic Risk, Pandemic Risk, Complex Systems, Risk Management for Networks.
MSC2020: 05C82, 05C90, 90B18, 91B05, 91G45, 93B70

1. Introduction

Modern societies and economies are increasingly dependent on systems that are characterized by complex forms of interconnectedness and interactions between different actors and system entities. Examples of such critical infrastructures are energy grids, transportation and communication systems, financial markets, and digital systems such as the internet.

However, the complexity of interaction channels also constitutes a major source of risk. The term *systemic risk* refers to the risk arising from a spread and amplification of adverse effects in a system due to contagion. Typically, the spread is triggered by some initial failure or disruption. Then the interconnectedness of the system entities facilitates the propagation of this risk, and amplifies the overall impact of the incident. Therefore, the study of systemic risk involves not only understanding the individual components of a network but also examining its pattern of interactions and feedback mechanisms.

Our main focus in this paper is management of *systemic cyber risk* which constitutes a significant part of the general exposure to cyber risk.[1] For illustration, let us recall two striking incidents in recent years which may be categorized as systemic cyber risk:

[1]See [6] for a distinction between *idiosyncratic*, *systematic*, and *systemic* cyber risks.

- WannaCry is a worm-type malware that emerged on a large scale in May 2017, primarily infecting Windows operating systems. Approximately 230,000 computer devices across more than 150 countries were infected. Being a ransomware, the worm encoded data on the compromised systems and insisted on a payment of $300. The consequence of this encryption was the loss of data and the rendering of IT systems in healthcare services and industry completely unusable. The assessed damage caused varies from hundreds of millions to four billion US dollars. The identification of "kill switch" significantly contributed to the containment of the incident.

- The NotPetya malware appeared in June 2017 and was primarily directed at Ukraine. Disguised as ransomware, this iteration of the Petya malware aimed not only to encrypt data but also to inflict maximum damage by disrupting IT systems. The data encryption led to an irreversible loss of accessibility, causing immediate repercussions for institutions like the Ukrainian Central Bank and significant disruptions in the country's major stock markets. Furthermore, the malware managed to infiltrate organizations beyond the Ukrainian financial sector that had offices in Ukraine, compromising machines in other countries as well. For instance, the global shipping company Maersk faced extensive business disruptions in various parts of the world.

One fundamental concept in understanding complex systems is the representation of their components and interactions as *networks*—a term which we use synonymously with *graphs*. The nodes of the network represent the individual entities, and edges depict the connections or relationships between them. In cyber systems, these nodes could be computers, servers, or even individual users, while financial systems might have nodes representing banks, markets, or financial investors. Possible interpretations of nodes and edges in electrical systems or in the case of a public transport system are also obvious.

We develop a conceptual framework for risk measures quantifying the resilience of networks to contagion and pandemic outbreak. To this end, we follow a well-established approach to risk assessment and base the risk measure on three main ingredients:

- a set $\mathcal{A}$ of acceptable networks which are deemed to have a sufficient degree of resilience to contagion,

- a set $\mathcal{I}$ of topological interventions to transform non-acceptable configurations into acceptable ones by altering the network structure,

- a quantification of the cost $\mathcal{C}$ (not necessarily in monetary terms) of making some network acceptable.

Naturally, there is an interplay between these three components, and they will account for the trade-off between functionality of the system, on the one hand, and interconnectedness as a major source for risk, on the other hand. Our findings may be relevant for different types of *supervisors*, such as

a) a *regulator* or *central planner* who aims to manage risk and resilience of (digital) systems and infrastructures from the perspective of a society. The need for a conceptual framework to manage systemic cyber risks has been widely discussed by leading regulatory or macroprudential institutions, see for example [24], [27], [28] and the discussion below.

b) an *insurance company* concerned with the limits of insurability of systemic accumulation risk and the design of policy exclusions. Insurers can also act as *private regulators* by requiring or incentivising security and system standards among their policyholders through contractual obligations, see the discussion in [5].

c) a *(local) risk manager* who is concerned with the network protection of a single firm or industry cluster.

Even though we will mostly limit our discussion to systemic cyber risks, especially in the axiomatization of acceptance sets $\mathcal{A}$, we want to emphasize that this risk management approach can also be applied to other forms of systemic risk, including those where the trade-off between functionality and risk due interconnectedness may be different from the cyber risk case. In electrical networks, for instance, an increase of interconnectedness may be desirable from the risk perspective—possibly avoiding blackouts.

A central feature of the risk measures for systemic risk we study in this paper is that a network is secured by allowing the risk manager to alter the network topology by means of topological interventions collected in the control set $\mathcal{I}$. There are a number of reasons for this approach:

First of all, it is well-known that the risk of a contagious spread is significantly determined by the topology of a network, as illustrated, for instance, in the analysis in [5]. To the best of our knowledge, existing works on systemic cyber risk typically model the risk control of networked actors via (individual) security levels or monetary investments, see the review on strategic interaction models for cyber risks in [6] and [53]. This security level or investment is a rather abstract variable whose increase is intended to somehow reduce the vulnerability to cyber attacks in an unspecified manner. In contrast, by allowing for topological interventions, we achieve more operational clarity as compared to most previous attempts, because the controls $\mathcal{I}$ come with a meaningful practical interpretation as outlined in Section 3.

Secondly, also in practice the discussion of security standards for interconnected systems increasingly focuses on the network structure. For example, in case of cyber security, regulators are increasingly pursuing a "Zero Trust" principle according to which no one is trusted by default from inside or outside the network. In particular no parts of a network are deemed to be more secure than other parts which implies that interactions with other entities of the network cannot be based, for instance, on the security standards of the other—this excludes, by the way, the aforementioned security levels and investments as controls. As a result, risk management is left with creating secure and resilient network architectures. For further information we refer to the discussion in [60] or in [55, Section 3.5.3].

Another example for the application of network models in practice is in the modelling of layered risks. For illustration consider the potential threat of cyber risks to financial stability, see [24], [27], [28]. Here network models are applied with a particular focus on the interplay between the operational cyber network and the financial network. So-called "cyber mappings" are used to identify systemically relevant network nodes in both the cyber network and the financial network and to analyse transmission channels of cyber risk to the financial system. A stylized illustration of a cyber map is given in Figure 1. These approaches are discussed, for example, in [14] and [28].

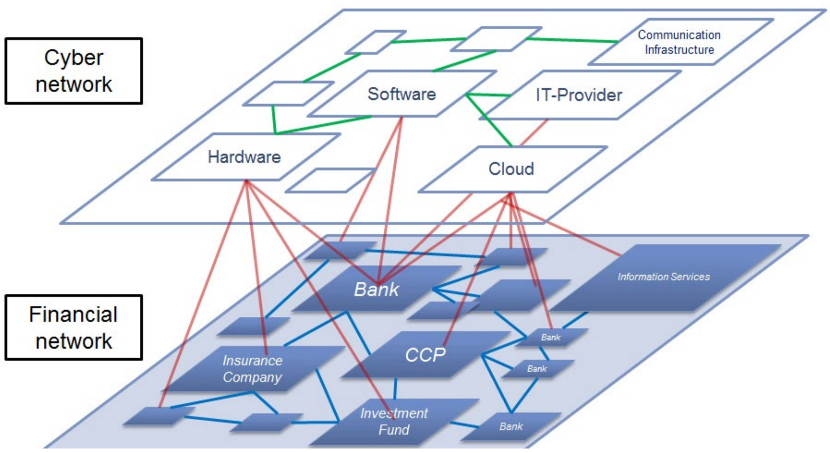

Figure 1: A stylized cyber map consisting of a cyber and a financial network. Taken from [28] and owned by Deutsche Bundesbank. Reproduced with permission.

Finally, from a theoretical perspective well-known results from dynamic models for network epidemics[2] suggests topological interventions (besides others) as appropriate controls to secure a network. Indeed, risk management strategies for systemic cyber risk which do not target the structure of the network are—in the framework of network epidemics—naturally interpreted as a change in the infection rate $\tau > 0$ and recovery rate $\gamma > 0$ of the contagion process, for instance due to an increased detection rate of system incidents, see [5]. A fundamental observation is that many real-world networks are characterized by a certain degree of heterogeneity, consisting of a small number of strongly connected entities, called *hubs*, and a vast majority of nodes with rather few adjacent neighbors. The distribution of node degrees, here represented by the random variable K_G, in these networks G typically follows a power law $\mathbb{P}(K_G = k) \sim k^{-\alpha}$, at least approximately. These so-called *scale-free networks* are commonly found among a wide range of social, technological, and information networks such as the internet, see Table 10.1 in [56].[3] Networks of this type are known to be highly vulnerable to pandemic contagion since infections of the hubs may immediately spread the risk to large parts of the system. For example, the phase transition behavior of the classical SIR (*Susceptible-Infected-Recovered*) network contagion model for undirected networks can be characterized in the limit of infinite network size by the epidemic threshold

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

see Chapter 6 in [50].[4] If (1) is satisfied, then epidemic outbreaks are possible; otherwise they are not. The crucial point is that in scale-free networks with $2 < \alpha \leq 3$, epidemic outbreaks are always possible, at least in the infinite size limit: For fixed values of the epidemic parameters τ and γ, which, we recall, would correspond to any non-topological risk controls, the left-hand side of (1) explodes with increasing network size due to the divergence of the second moment $\mathbb{E}[K_G^2]$ of the degree distribution while the first moment $\mathbb{E}[K_G]$ remains finite. Thus, taking the infinite size limit as an approximation of very large and expanding systems such as the internet, if we are not willing to touch the network topology, their protection may require huge and probably extremely expensive resources for a sufficient reduction of τ and increase of γ to avoid epidemic outbreaks, if at all possible.

Of course, altering the network structure may come at the cost of loosing functionality. This is where the cost function $\mathcal{C}$ comes into play. Apart from monetary costs of network interventions, measures of network functionality constitute an important class of cost functions, see Section 5. Together with the right choice of acceptance set $\mathcal{A}$ this allows to maintain a desired degree of network functionality while improving the networks resilience by interventions in $\mathcal{I}$.

Throughout the paper we will mention numerous open problems and questions which could serve as basis for future research. Some major topics are collected in the outlook Section 8. Even if some of the issues mentioned can be readily solved, we will have to leave them aside for the moment, since the purpose of this paper is to establish a framework for measures of resilience to cyber contagion, and we want to avoid escalating discussions of partial aspects.

Literature As regards the mathematical literature on cyber risk, we refer to the surveys [6] and [26] for a comprehensive overview. A few recent studies focusing on cyber insurance

[2]These processes which originate from the study of biological epidemics are frequently applied to model the systemic spread of cyber risk, see the discussion in the literature section below.

[3]A possible explanation for this phenomenon can be found in the random network models of [58], [59] and [8] based on the interplay of *network growth* and *cumulative advantage* or *preferential attachment*, i.e., the tendency of newly added network actors to connect with already highly interconnected nodes due to efficiency reasons.

[4]The threshold is exact for networks without additional correlation effects such as clustering or degree correlations. For an arbitrary degree distribution, such networks can, e.g., be generated using the *configuration model* from [54]. The influence of node degree correlations and clustering on epidemic dynamics is summarized in Section VII, B of [57]. Numerical and analytical work shows that these are not able to restore a finite threshold for scale-free networks, or at most in the case of very strong presence.

are [7], [10], [13], [20], [21], [44], [66], [67], and [68]. There is an increasing line of literature utilizing epidemic processes on networks known from theoretical biology (see, e.g. [50, 57]) to model the spread of contagious cyber risks in digital systems, see [2], [19], [31], [42], [43], [49], and [65]. The latter articles are mostly concerned with the pricing of cyber insurance policies. Further considerations on the significance of systemic cyber risks for the vulnerability of digitally networked societies and economies can be found in [38] and [64].

Systemic risk has long been studied in the context of financial systems, see for instance [39], [47], and [48] for an overview. In particular, models for contagion effects in financial networks have been proposed and studied in [1], [22], [25], and [40], whereas, for example, [3], [11], [17], [35], [34], [45], and [46] consider risk measures for systemic risk in financial markets. Applications of this type of risk measures outside the financial market frame are in transmission systems ([16]), for infrastructures ([61]), or traffic networks ([32]). However, non of these approaches directly targets the underlying network structure, see the discussion above.

An axiomatic approach to monetary risk measures goes back to [4], see also [36] and [37] for an overview of the theory on monetary risk measures. It is from this theory that we adopt the idea to base the risk assessment on a set of acceptable configurations $\mathcal{A}$, a set of controls $\mathcal{I}$, and related costs $\mathcal{C}$.

Outline After introducing the formalisation of networks and some related basic definitions in Section 2, we will first discuss network manipulations $\mathcal{I}$ in Section 3, then introduce acceptance sets $\mathcal{A}$ in Section 4, and finally consider the cost $\mathcal{C}$ of acceptability in Section 5. These components are merged into what we call a measure of resilience to cyber contagion in Section 6. Selected examples are given in Section 7. Section 8 provides an outlook on open problems for future research. Finally, the appendix contains some further examples and considerations for undirected graphs which are not discussed in the main part of the paper.

2. Networks - Basic Definitions

2.1. Graphs and Networks

A *graph* G is an ordered pair of sets $G = (\mathcal{V}_G, \mathcal{E}_G)$ where $\mathcal{V}_G$ is a set of elements, called *nodes* (or *vertices*), and $\mathcal{E}_G \subseteq \mathcal{V}_G \times \mathcal{V}_G$ a set of pairs, called *edges* (or *links*). In the following, we will always assume $(v, v) \notin \mathcal{E}_G$, i.e, we do not allow for self-connections of nodes. Further, for the rest of the paper, we assume that all graphs are defined over the same non-empty countably infinite basis set of nodes $\mathbb{V}$, i.e., that $\mathcal{V}_G \subseteq \mathbb{V}$ for all graphs G. We denote the set of such graphs by

$$\mathcal{G} := \{G \mid G = (\mathcal{V}_G, \mathcal{E}_G), \mathcal{V}_G \subset \mathbb{V}, \mathcal{E}_G \subset (\mathcal{V}_G \times \mathcal{V}_G) \cap \mathbb{E}\}$$

where $\mathbb{E} := \{(v, w) \in \mathbb{V} \times \mathbb{V} \mid v \neq w\}$. $|\mathcal{V}_G|$ is called the *size* of graph G. A graph $G' = (\mathcal{V}', \mathcal{E}')$ with $\mathcal{V}' \subseteq \mathcal{V}_G$, $\mathcal{E}' \subseteq \mathcal{E}_G$ is called a *subgraph* of G.

A *network* is any structure which admits an abstract representation as a graph: The nodes represent the network's agents or entities, while the connecting edges correspond to a relation or interaction among those entities. In the following, we use the terms "graph" and "network" interchangeably.

An important subclass of $\mathcal{G}$ are the so-called *undirected graphs*: A graph $G \in \mathcal{G}$ is called *undirected* if for all $v, w \in \mathcal{V}_G$ we have $(v, w) \in \mathcal{E}_G \;\Leftrightarrow\; (w, v) \in \mathcal{E}_G$. A graph which is not undirected is often referred to as being *directed*. There is a vast literature on undirected graphs and popular network models restrict themselves to this subclass. However, throughout this paper we will work with the complete set of directed graphs $\mathcal{G}$ since the direction of a possible information flow may be essential to understand the associated risk of a corresponding connection. Nevertheless, our results, or appropriate versions of the results, also hold if we restrict ourselves to the undirected case, see Appendix B for the details. Moreover, in Appendices B.2.3 and B.2.6 we provide examples which are peculiar to an undirected graph framework.

An extension of $\mathcal{G}$ is obtained through the incorporation of *weights* assigned to the edges, symbolizing the extent of transmissibility of a shock across each respective edge. Nonetheless, defining the precise nature and magnitude of these weights might pose a challenge. We briefly discuss the enhancement of our framework to weighted graphs in the outlook Section 8.

2.2. Adjacency Matrix

For a network of size N, the nodes can be enumerated, say as $v_1, \cdots, v_N$. Given an enumeration of the vertex set $\mathcal{V}_G$, the *network topology*, i.e., the spatial pattern of interconnections, of a network G is described by its *adjacency matrix* $A_G = (A_G(i,j))_{i,j=1,\cdots,N} \in \{0,1\}^{N\times N}$, where

$$A_G(i,j) = \begin{cases} 1, & \text{if } (v_i, v_j) \in \mathcal{E}_G \\ 0, & \text{else.} \end{cases}$$

Note that G is undirected if and only if A_G is a symmetric matrix.

2.3. Neighborhoods of Nodes and Node Degrees

For a graph $G = (\mathcal{V}_G, \mathcal{E}_G)$ and node $v \in \mathcal{V}_G$, we define $\mathcal{N}_v^{G,in} := \{w \in \mathcal{V}_G | (w,v) \in \mathcal{E}_G\}$ and $\mathcal{N}_v^{G,out} := \{w \in \mathcal{V}_G | (v,w) \in \mathcal{E}_G\}$ as the *in-* and *out-neighborhoods* of node v. The *neighborhood* is $\mathcal{N}_v^G := \mathcal{N}_v^{G,in} \cup \mathcal{N}_v^{G,out}$. A network G is undirected if and only if $\mathcal{N}_v^{G,in} = \mathcal{N}_v^{G,out} = \mathcal{N}_v^G$ for all $v \in \mathcal{V}_G$. The set $\mathcal{E}_G^v := \{(u,w) \in \mathcal{E}_G | u = v \text{ or } w = v\}$ contains all edges associated with node v in graph G.

In order to characterize and quantify structural differences between network nodes, a possible way is to measure the number of adjacent neighbors, i.e., with how many others a node is connected. The *incoming* or *in-degree*, i.e., the number of edges arriving at node v, is defined as $k_v^{G,in} = |\mathcal{N}_v^{G,in}|$, and the *outgoing* or *out-degree* as $k_v^{G,out} = |\mathcal{N}_v^{G,out}|$. For some enumeration $v_1, \ldots, v_N$ of $\mathcal{V}_G$, these entities can be expressed in terms of the adjacency matrix A_G by

$$k_{v_i}^{G,in} = \sum_{j=1}^{N} A_G(j,i), \qquad k_{v_i}^{G,out} = \sum_{j=1}^{N} A_G(i,j).$$

The *(total) degree* k_v^G of node v in network G is defined as

$$k_v^G = \frac{1}{2}(k_v^{G,in} + k_v^{G,out}).$$

Typically, total degrees are studied in the context of undirected networks G where we find that $k_v^G = k_v^{G,in} = k_v^{G,out}$ due to the fact that $\mathcal{N}_v^{G,out} = \mathcal{N}_v^{G,in}$ for all $v \in \mathcal{V}_G$.

2.4. Walks, Paths, and Connectivity of Graphs

Given a graph G, a *walk* of length n from node v to node w in G is an $(n+1)$-tuple of nodes $(v_1, v_2, \ldots, v_{n+1})$ such that $(v_i, v_{i+1}) \in \mathcal{E}_G$ for all $1 \le i \le n$ and $v_1 = v$ and $v_{n+1} = w$. A *path* from v to w is a walk where all nodes are distinct.

A graph G is called *(weakly) connected* if there exists a path from v to w or from w to v for any two nodes $v, w \in \mathcal{V}_G$. A *component* $\tilde{G}$ of network G is a weakly connected subgraph, and two components $G_1 = (\mathcal{V}_1, \mathcal{E}_1)$, $G_2 = (\mathcal{V}_1, \mathcal{E}_2)$ of G are called *disconnected* if there are no $v \in \mathcal{V}_1$ and $w \in \mathcal{V}_2$ such that there is a path from v to w or from w to v in G. A graph G is called *strongly connected* if for each node pair $v, w \in \mathcal{V}_G$ there exist paths from v to w and from w to v.

2.5. Equivalence Classes of Isomorphic Graphs

Two graphs $G_1 = (\mathcal{V}_1, \mathcal{E}_1), G_2 = (\mathcal{V}_2, \mathcal{E}_2) \in \mathcal{G}$ share the same topology if there is a bijection $\pi : \mathcal{V}_1 \to \mathcal{V}_2$ such that

$$(v, w) \in \mathcal{E}_1 \Leftrightarrow (\pi(v), \pi(w)) \in \mathcal{E}_2 \text{ for all } v, w \in \mathcal{V}_1.$$

π is called a *graph isomorphism* of G_1 and G_2, and we write $G_1 \overset{iso}{\sim} G_2$. Clearly, given a graph $G_1 = (\mathcal{V}_1, \mathcal{E}_1)$ any bijection $\pi : \mathcal{V}_1 \to \mathcal{V}_2$ where $\mathcal{V}_2 \subset \mathbb{V}$ defines a graph $\pi(G) = (\mathcal{V}_2, \mathcal{E}_2)$ where $\mathcal{E}_2 = \{(\pi(v), \pi(w)) \mid v, w \in \mathcal{V}_1\}$ called an *isomorphism of* G or *the isomorphism of* G *under* π. $\overset{iso}{\sim}$ is an equivalence relation on $\mathcal{G}$.

3. Network Interventions

Definition 3.1. *A* ***network intervention*** *is a map* $\kappa : \mathcal{G} \to \mathcal{G}$.

3.1. Basic Interventions

In this section we introduce some basic types of interventions on graphs $G = (\mathcal{V}_G, \mathcal{E}_G) \in \mathcal{G}$. These manipulations have also previously been applied in the literature on network risk management, see e.g. [5] and [18] for the case of cyber networks.

3.1.1. Elementary Interventions on Edges and Nodes

$\mathcal{I}_{e\_del}$ **Edge Deletion**: Consider a node tuple (v, w), $v, w \in \mathbb{V}$. The operation

$$\kappa^{(v,w)}_{e\_del} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \setminus \{(v, w)\})$$

is called the deletion of edge (v, w). Note that $\kappa^{(v,w)}_{e\_del}(G) = G$ if and only if $(v, w) \notin \mathcal{E}_G$. We set

$$\mathcal{I}_{e\_del} := \{\kappa^{(v,w)}_{e\_del} \mid v, w \in \mathbb{V}\}.$$

Operational interpretations of edge deletion for controlling cyber risk are

- *physical deletion of connections*, such as access to servers, or, if not possible,
- *edge hardening*, i.e., a strong protection of network connections via firewalls, the closing of open ports, or the monitoring of data flows using specific detection systems.

$\mathcal{I}_{e\_add}$ **Edge Addition**: The addition of edge (v, w) for $v, w \in \mathbb{V}$ with $v \neq w$ is given by

$$\kappa^{(v,w)}_{e\_add} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \cup (\{(v, w)\} \cap \mathcal{V}_G \times \mathcal{V}_G)),$$

where $\kappa^{(v,w)}_{e\_add}(G) = G$ is satisfied if either we already have $(v, w) \in \mathcal{E}_G$ or at least one of the nodes v and w is not present in the network G. We set

$$\mathcal{I}_{e\_add} := \{\kappa^{(v,w)}_{e\_add} \mid v, w \in \mathbb{V}\}.$$

Edge addition is, of course, the reverse of edge deletion and comes with the opposite operational meaning. In the context of electrical networks, edge addition may be interpreted as physical addition of power lines between nodes, thereby securing power supply.

$\mathcal{I}_{n\_del}$ **Node Deletion**: The deletion of a node $v \in \mathbb{V}$ is given by the intervention

$$\kappa^{v}_{n\_del} : G \mapsto (\mathcal{V}_G \setminus \{v\}, \mathcal{E}_G \cap (\mathcal{V}_G \setminus \{v\} \times \mathcal{V}_G \setminus \{v\}))$$

where $\kappa^v_{n\_del}(G) = G$ if and only if $v \notin \mathcal{V}_G$. We set

$$\mathcal{I}_{n\_del} := \{\kappa^v_{n\_del} \mid v \in \mathbb{V}\}.$$

Operationally node deletion corresponds, for instance, to removal of redundant servers or other access points.

$\mathcal{I}_{n\_add}$ **Node Addition**: An (isolated) node $v \in \mathbb{V}$ can be added to a network via

$$\kappa^v_{n\_add} : G \mapsto (\mathcal{V}_G \cup \{v\}, \mathcal{E}_G)$$

where $\kappa^v_{n\_add}(G) = G$ if and only if we already have $v \in \mathcal{V}_G$. We set

$$\mathcal{I}_{n\_add} := \{\kappa^v_{n\_add} \mid v \in \mathbb{V}\}.$$

Node addition, e.g. additional servers serving as backups or taking over tasks from very central servers, my improve network resilience towards a spread of infectious software if combined with edge addition or edge shifts, see below.

More complex interventions such as discussed in the following can be obtained by a consecutive application of the elementary interventions presented so far.

3.1.2. Isolation of Network Parts

Critical nodes or subgraphs can be isolated from the rest of the network by application of the following edge deletion procedures:

$\mathcal{I}_{s\_iso}$ **Node/Subgraph Isolation**: We isolate the subgraph $(\mathcal{W} \cap \mathcal{V}_G, \mathcal{E}_G \cap (\mathcal{W} \times \mathcal{W}))$ given by a set $\mathcal{W} \subset \mathbb{V}$ (or a node in case $\mathcal{W} = \{v\}$ for some $v \in \mathbb{V}$) from the rest of the network by

$$\kappa^{\mathcal{W}}_{iso} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \setminus [\mathcal{W} \times (\mathcal{V}_G \setminus \mathcal{W}) \cup (\mathcal{V}_G \setminus \mathcal{W}) \times \mathcal{W}]), \quad \mathcal{I}_{s\_iso} := \{\kappa^{\mathcal{W}}_{iso} \mid \mathcal{W} \subset \mathbb{V}\}.$$

3.1.3. Shifting, Diversification and Centralization of Network Connections

Network tasks or data flows can be redistributed among existing nodes by utilizing interventions of the following type:

$\mathcal{I}_{shift}$ **Edge Shift**: If $(v, w) \in \mathcal{E}_G$ and $(q, r) \in \mathbb{E} \setminus \mathcal{E}_G$, $q, r \in \mathcal{V}_G$, then the edge (v, w) can be shifted to (q, r) by

$$\kappa^{(v,w),(q,r)}_{shift} : G \mapsto \begin{cases} (\mathcal{V}_G, \mathcal{E}_G \setminus \{(v, w)\} \cup \{(q, r)\}), & \textit{if } (v, w) \in \mathcal{E}_G, q, r \in \mathcal{V}_G, (q, r) \in \mathbb{E} \setminus \mathcal{E}_G \\ G, & \textit{else.} \end{cases}$$

We set

$$\mathcal{I}_{shift} := \{\kappa^{(v,w),(q,r)}_{shift} \mid v, w, q, r \in \mathbb{V}\}.$$

Combining node adding and edge shift operations, we can create more complex interventions which aim for risk diversification by separating critical contagion channels that pass through a chosen node v:[5]

[5]Note that a reduction of paths by splitting of v is only possible if $\mathcal{N}^{G,out}_v, \mathcal{N}^{G,in}_v \neq \emptyset$. Further, let $\tilde{G} = \kappa^{\mathcal{L},v,\tilde{v}}_{split}(G)$. An actual reduction of paths in $\tilde{G}$ is obtained in case that $\mathcal{N}^{\tilde{G},in}_v$, $\mathcal{N}^{\tilde{G},out}_{\tilde{v}} \neq \emptyset$, or $\mathcal{N}^{\tilde{G},out}_v$, $\mathcal{N}^{\tilde{G},in}_{\tilde{v}} \neq \emptyset$.

$\mathcal{I}_{split}$ **Node Splitting**: The split of a node v by rewiring edges contained in $\mathcal{L} \subset \mathbb{E}$ from v to a newly added node $\tilde{v} \in \mathbb{V}$ is described by

$$\kappa_{split}^{\mathcal{L},v,\tilde{v}} : G \mapsto \begin{cases} (\mathcal{V}_G \cup \{\tilde{v}\}, \mathcal{E}_G \setminus (\mathcal{L} \cap \mathcal{E}_G^v) \cup \tilde{\mathcal{L}}_{\tilde{v}}^G), & \text{if } \tilde{v} \notin \mathcal{V}_G \\ G, & \text{else,} \end{cases}$$

with $\tilde{\mathcal{L}}_{\tilde{v}}^G := \{(\tilde{v}, w) | (v, w) \in \mathcal{L} \cap \mathcal{E}_G\} \cup \{(w, \tilde{v}) | (w, v) \in \mathcal{L} \cap \mathcal{E}_G\}$. A true node splitting only takes place when $\tilde{v} \notin \mathcal{V}_G$ and $\mathcal{L} \cap \mathcal{E}_G^v \neq \emptyset$. Let

$$\mathcal{I}_{split} := \{\kappa_{split}^{\mathcal{L},v,\tilde{v}} \mid v, \tilde{v} \in \mathbb{V}, \mathcal{L} \subset \mathbb{E}\}.$$

Conversely, node splits can be reversed by *merging* nodes v and $\tilde{v}$. This operation corresponds to a centralization of network connections:

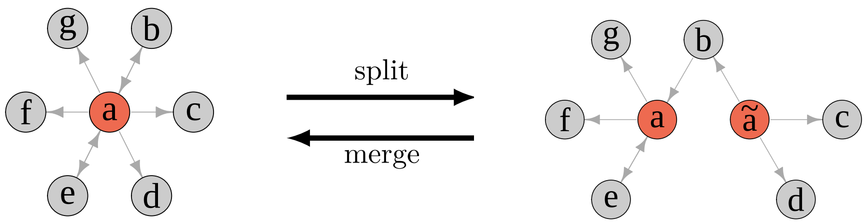

Figure 2: Splitting (left to right) and merging (right to left) as mutually reverse operations. Targeted nodes are coloured in red.

$\mathcal{I}_{merge}$ **Node Merging**: Any two nodes v, w with $(v, w), (w, v) \notin \mathcal{E}_G$ which are of disjoint in- and out-neighborhood can properly be merged into node v. This corresponds to the intervention

$$\kappa_{merge}^{v,w} : G \mapsto \begin{cases} (\mathcal{V}_G \setminus \{w\},\ (\mathcal{E}_G \setminus \mathcal{E}_G^w) \cup \mathcal{M}_G), & \text{if } v, w \in \mathcal{V}_G, \{(v,w),(w,v)\} \cap \mathcal{E}_G = \emptyset, \\ & \mathcal{N}_v^{G,in} \cap \mathcal{N}_w^{G,in} = \mathcal{N}_v^{G,out} \cap \mathcal{N}_w^{G,out} = \emptyset \\ G, & \text{else,} \end{cases}$$

with $\mathcal{M}_G := \{(v, q) | q \in \mathcal{N}_w^{G,out}\} \cup \{(q, v) | q \in \mathcal{N}_w^{G,in}\}$. Let

$$\mathcal{I}_{merge} := \{\kappa_{merge}^{v,w} \mid v, w \in \mathbb{V}\}.$$

3.2. Strategies, Reverse and Orthogonal Sets of Interventions

Definition 3.2. *Given a set $\mathcal{I}$ of interventions defined on $\mathcal{G}$, an ($\mathcal{I}$-)**strategy** κ is a finite composition of interventions in $\mathcal{I}$, i.e. $\kappa = \kappa_1 \circ \ldots \circ \kappa_n$ where $\kappa_i \in \mathcal{I}$ for all $i = 1, \ldots, n$ and $n \in \mathbb{N}$. We let $[\mathcal{I}]$ denote the set consisting of all $\mathcal{I}$-strategies, and in addition, if not already included in $\mathcal{I}$, the intervention* $\mathrm{id} : G \mapsto G$.

Definition 3.3. *Let $\mathcal{I}$, $\mathcal{J}$ be sets of network interventions on $\mathcal{G}$.*

1. *We call $\mathcal{J}$ a **reversion** of $\mathcal{I}$, written $\mathcal{J} \triangleright \mathcal{I}$, if for every $\alpha \in \mathcal{I}$ and network $G \in \mathcal{G}$ we find a $\kappa \in [\mathcal{J}]$ such that $\kappa \circ \alpha(G) = G$.*

2. *If $\mathcal{J} \triangleright \mathcal{I}$ and $\mathcal{I} \triangleright \mathcal{J}$, then we write $\mathcal{I} \triangle \mathcal{J}$ and call $\mathcal{I}$ and $\mathcal{J}$ **mutually reverse**.*

3. *We call $\mathcal{I}$ **self-reverse** if $\mathcal{I} \triangleright \mathcal{I}$ (or, equivalently, $\mathcal{I} \triangle \mathcal{I}$).*

4. *$\mathcal{J}$ is a* ***partial reversion*** *of $\mathcal{I}$ if there is $G \in \mathcal{G}$, a $\alpha \in [\mathcal{I}]$ with $\alpha(G) \neq G$, and a $\kappa \in [\mathcal{J}]$ such that $\kappa \circ \alpha(G) = G$. In case $\mathcal{I}$ is a partial reversion of itself, we call $\mathcal{I}$* ***partially self-reverse****.*

Note that the reversions $\kappa \in \mathcal{J}$ such that $\kappa \circ \alpha(G) = G$ in the above definitions may depend on G.

Lemma 3.4. 1. *$\mathcal{J} \triangleright \mathcal{I}$ if and only if $[\mathcal{J}] \triangleright [\mathcal{I}]$.*

2. *If $\mathcal{I} \triangleright \mathcal{J}$, $\mathcal{J} \triangleright \mathcal{K}$, and $\mathcal{K} \triangleright \mathcal{L}$, then we also have $\mathcal{I} \triangleright \mathcal{L}$.*

3. *If $\mathcal{I} \triangleright \mathcal{J}$ and $\mathcal{H} \triangleright \mathcal{K}$, then $(\mathcal{I} \cup \mathcal{H}) \triangleright (\mathcal{J} \cup \mathcal{K})$.*

4. *The relation $\triangle$ is a symmetric. Moreover, 1.,2.,3. hold with $\triangleright$ replaced by $\triangle$.*

Proof. 1. Suppose that $\mathcal{J} \triangleright \mathcal{I}$ and let $\alpha = \alpha_1 \circ \cdots \circ \alpha_n$ where $\alpha_i \in \mathcal{I}$, $i = 1, \ldots, n$. Further, let $\kappa_i \in [\mathcal{J}]$ such that $\kappa_n \circ \alpha_n(G) = G$, and $\kappa_i \circ \alpha_i(\alpha_{i+1} \circ \ldots \circ \alpha_n(G)) = \alpha_{i+1} \circ \ldots \circ \alpha_n(G)$, $i = 1, \ldots, n-1$. Then $\kappa = \kappa_n \circ \cdots \circ \kappa_1 \in [\mathcal{J}]$ satisfies $\kappa \circ \alpha(G) = G$. If $[\mathcal{J}] \triangleright [\mathcal{I}]$, then $\mathcal{J} \triangleright \mathcal{I}$ since $\mathcal{I} \subset [\mathcal{I}]$ and $[[\mathcal{J}]] = [\mathcal{J}]$.
2. Let $\kappa_{\mathcal{L}} \in \mathcal{L}$ and choose $\kappa_{\mathcal{I}} \in \mathcal{I}$, $\kappa_{\mathcal{J}} \in \mathcal{J}$, and $\kappa_{\mathcal{K}} \in \mathcal{K}$ such that $\kappa_{\mathcal{K}} \circ \kappa_{\mathcal{L}}(G) = G$, $\kappa_{\mathcal{J}} \circ \kappa_{\mathcal{K}} \circ \kappa_{\mathcal{L}}(G) = \kappa_{\mathcal{L}}(G)$, and $\kappa_{\mathcal{I}} \circ \kappa_{\mathcal{J}}(G) = G$. Then $G = \kappa_{\mathcal{I}} \circ \kappa_{\mathcal{J}} \circ \kappa_{\mathcal{K}} \circ \kappa_{\mathcal{L}}(G) = \kappa_{\mathcal{I}} \circ \kappa_{\mathcal{L}}(G)$.
3. is obvious.
4. The first assertion is clear. The others follow from symmetry and 1.,2.,3. □

We introduce another concept that specifies whether consecutive interventions from $\mathcal{I}$ and $\mathcal{J}$ can generate the same output when applied to an initial network $G \in \mathcal{G}$:

Definition 3.5. *Two sets $\mathcal{I}$, $\mathcal{J}$ of network interventions are called* ***orthogonal****, $\mathcal{I} \perp \mathcal{J}$, if for all $G \in \mathcal{G}$ and all $\kappa \in [\mathcal{I}]$ and $\tilde{\kappa} \in [\mathcal{J}]$ we have $\kappa(G) = \tilde{\kappa}(G)$ if and only if $\kappa(G) = G = \tilde{\kappa}(G)$.*

Remark 3.6. *A sufficient condition for $\mathcal{I} \perp \mathcal{J}$ is that $|\mathcal{V}_{\kappa(G)}| \neq |\mathcal{V}_{\tilde{\kappa}(G)}|$ or $|\mathcal{E}_{\kappa(G)}| \neq |\mathcal{E}_{\tilde{\kappa}(G)}|$ for all $\kappa \in [\mathcal{I}]$ and $\tilde{\kappa} \in [\mathcal{J}]$ whenever we have $\kappa(G) \neq G$ or $\tilde{\kappa}(G) \neq G$. This is especially the case when the two types of network interventions are opposite in terms of change of the number of nodes or edges.*

Example 3.7. *The relations between the previously introduced types of basic interventions can be characterized in terms of reversibility and orthogonality:*

1. *For reversibility, we find*
   - *$\mathcal{I}_{e\_del} \triangle \mathcal{I}_{e\_add}$ and $\mathcal{I}_{split} \triangle \mathcal{I}_{merge}$, and these are the only two classes of basic interventions that are mutually reverse.*
   - *$\mathcal{I}_{shift}$ is the only self-reverse basic intervention class.*
   - *$\mathcal{I}_{e\_add} \triangleright \mathcal{I}_{s\_iso}$ and $\mathcal{I}_{n\_del} \triangleright \mathcal{I}_{n\_add}$, but the converse results do not apply.*

2. *Recalling Remark 3.6 we observe that*
   - *all elementary interventions are pairwise orthogonal, i.e., we have $\mathcal{I}_{e\_del} \perp \mathcal{I}_{e\_add}$, $\mathcal{I}_{e\_del} \perp \mathcal{I}_{n\_del}$, $\mathcal{I}_{e\_del} \perp \mathcal{I}_{n\_add}$, $\mathcal{I}_{e\_add} \perp \mathcal{I}_{n\_del}$, $\mathcal{I}_{e\_add} \perp \mathcal{I}_{n\_add}$, and $\mathcal{I}_{n\_del} \perp \mathcal{I}_{n\_add}$,*
   - *$\mathcal{I}_{shift}$ is the only basic intervention class where for a real network manipulation $\kappa(G) \neq G$ the number of edges or nodes remains unaffected, and consequently, it is orthogonal to all other classes of basic interventions,*
   - *we further have $\mathcal{I}_{split} \perp \mathcal{I}_{merge}$, $\mathcal{I}_{split} \perp \mathcal{I}_{e\_del}$, $\mathcal{I}_{split} \perp \mathcal{I}_{e\_add}$, $\mathcal{I}_{split} \perp \mathcal{I}_{n\_del}$, $\mathcal{I}_{merge} \perp \mathcal{I}_{e\_del}$, $\mathcal{I}_{merge} \perp \mathcal{I}_{e\_add}$, and $\mathcal{I}_{merge} \perp \mathcal{I}_{n\_add}$.*
   - *For each set $\mathcal{I}$ with $\mathcal{I} \perp \mathcal{I}_{e\_del}$, we also have $\mathcal{I} \perp \mathcal{I}_{s\_iso}$.*

3. *The relations in 1. and 2. remain valid whenever we restrict the network interventions to subsets of nodes and edges. Of course, in case of $\triangleright$ and $\triangle$ the restriction has to be consistent on both sides. In practice, the interventions available to a supervisor may indeed be constrained to such subsets, see also Remark 6.3 below.*

Lemma 3.8. *Let $\mathcal{I}$ and $\mathcal{J}$ be mutually reverse. Then the following statements are equivalent:*

1. *$\mathcal{I}$ and $\mathcal{J}$ are orthogonal.*

2. *Either $\mathcal{I}$ or $\mathcal{J}$ is not partially self-reverse.*

3. *Both $\mathcal{I}$ or $\mathcal{J}$ are not partially self-reverse.*

Proof. Clearly, 3. $\Rightarrow$ 2.

1. $\Rightarrow$ 3.: Assume that $\mathcal{I}$ is a partially self-reverse. Then, there is $G \in \mathcal{G}$ and strategies $\kappa, \tilde{\kappa} \in [\mathcal{I}]$ such that $\tilde{\kappa} \circ \kappa(G) = G$ with $H := \kappa(G) \neq G$. Now, since $\mathcal{J} \triangleright \mathcal{I}$, we find a $\mathcal{J}$-strategy $\hat{\kappa}$ with $\hat{\kappa} \circ \tilde{\kappa}(H) = H$, according to Lemma 3.4. Therefore, we have $\hat{\kappa}(G) = \kappa(G) \neq G$, and this implies that $\mathcal{I}$ and $\mathcal{J}$ are not orthogonal which contradicts 1. Hence, $\mathcal{I}$ cannot be partially self-reverse. The assertion now follows from interchanging the roles of $\mathcal{I}$ and $\mathcal{J}$.

2. $\Rightarrow$ 1.: Suppose $\mathcal{I}$ and $\mathcal{J}$ are not orthogonal. Then we find a network $G \in \mathcal{G}$ and consecutive interventions $\kappa \in [\mathcal{I}]$, $\tilde{\kappa} \in [\mathcal{J}]$ such that $\kappa(G) = \tilde{\kappa}(G) \neq G$. Now, since $\mathcal{I}$ is a reversion of $\mathcal{J}$, we find a $\hat{\kappa} \in [\mathcal{I}]$ with $G = \hat{\kappa} \circ \tilde{\kappa}(G) = \hat{\kappa} \circ \kappa(G)$, and therefore, $\mathcal{I}$ is a partial reversion of itself. The same argument applies to $\mathcal{J}$ which contradicts 2. Hence, $\mathcal{I}$ and $\mathcal{J}$ must be orthogonal.

$\square$

3.3. Generation of Networks Using Interventions

Consider a given network $G \in \mathcal{G}$ and a set of interventions $\mathcal{I}$ on $\mathcal{G}$. The set

$$\sigma^{\mathcal{I}}(G) := \{\kappa(G) | \kappa \in [\mathcal{I}]\}$$

contains all networks $\tilde{G} \in \mathcal{G}$ that can be generated from G under consecutive interventions built from $\mathcal{I}$. Note that we always have $G \in \sigma^{\mathcal{I}}(G)$ due to id $\in [\mathcal{I}]$. Using the concepts from the previous subsection, we can characterize the relation between sets $\sigma^{\mathcal{I}}(G)$ and $\sigma^{\mathcal{J}}(G)$ for two sets of interventions $\mathcal{I}$ and $\mathcal{J}$:

Proposition 3.9. *Let $\mathcal{I}$, $\mathcal{J}$ be sets of interventions on $\mathcal{G}$.*

1. *For all $G, H \in \mathcal{G}$, $H \in \sigma^{\mathcal{I}}(G)$ implies $\sigma^{\mathcal{I}}(H) \subseteq \sigma^{\mathcal{I}}(G)$.*

2. *Suppose that $\mathcal{I}$ is not partially self-reverse. Then*
$$G \preccurlyeq_{\mathcal{I}} H \quad :\Leftrightarrow \quad H \in \sigma^{\mathcal{I}}(G)$$
defines a partial order on $\mathcal{G}$.

3. *$\mathcal{J} \triangleright \mathcal{I}$ holds if and only if we have that $H \in \sigma^{\mathcal{I}}(G) \Rightarrow G \in \sigma^{\mathcal{J}}(H)$ for all $G, H \in \mathcal{G}$. In particular, we have $\mathcal{I} \triangle \mathcal{J}$ if and only if $H \in \sigma^{\mathcal{I}}(G) \Leftrightarrow G \in \sigma^{\mathcal{J}}(H)$ for all $G, H \in \mathcal{G}$.*

4. *$\mathcal{I} \perp \mathcal{J}$ if and only if $\sigma^{\mathcal{I}}(G) \cap \sigma^{\mathcal{J}}(G) = \{G\}$ for all $G \in \mathcal{G}$.*

5. *Let $\mathcal{K} = \mathcal{I}_{e\_del} \cup \mathcal{I}_{e\_add} \cup \mathcal{I}_{n\_del} \cup \mathcal{I}_{n\_add}$ be the set that contains all elementary interventions from Section 3.1.1. Then $\sigma^{\mathcal{K}}(G) = \mathcal{G}$ for all $G \in \mathcal{G}$.*

Proof. 1. For $H \in \sigma^{\mathcal{I}}(G)$ and an arbitrary $L \in \sigma^{\mathcal{I}}(H)$, we find $\kappa, \tilde{\kappa} \in [\mathcal{I}]$ with $\kappa(G) = H$, and $\tilde{\kappa}(H) = L$, respectively. Then $\tilde{\kappa} \circ \kappa \in [\mathcal{I}]$ and $\tilde{\kappa} \circ \kappa(G) = L$, so that $L \in \sigma^{\mathcal{I}}(G)$.

2. id $\in [\mathcal{I}]$ implies reflexivity, and transitivity follows from 1. Finally suppose that $G \preccurlyeq_{\mathcal{I}} H$ and $H \preccurlyeq_{\mathcal{I}} G$, then there are $\mathcal{I}$-strategies $\kappa, \tilde{\kappa}$ such that $H = \kappa(G)$ and $G = \tilde{\kappa}(H) = \tilde{\kappa} \circ \kappa(G)$. Since $\mathcal{I}$ is not partially self-reverse, we must have $H = \kappa(G) = G$. This proves antisymmetry of $\preccurlyeq_{\mathcal{I}}$.

3. Let $H \in \sigma^{\mathcal{I}}(G)$ and $\kappa \in [\mathcal{I}]$ with $H = \kappa(G)$. If $\mathcal{J} \rhd \mathcal{I}$, then by Lemma 3.4 we can find a $\tilde{\kappa} \in [\mathcal{J}]$ with $G = \tilde{\kappa} \circ \kappa(G) = \tilde{\kappa}(H) \in \sigma^{\mathcal{J}}(H)$. Conversely, suppose that $H \in \sigma^{\mathcal{I}}(G) \Rightarrow G \in \sigma^{\mathcal{J}}(H)$ for all $G, H \in \mathcal{G}$. This means that for all $G \in \mathcal{G}$ and $\kappa \in [\mathcal{I}]$, we find a $\tilde{\kappa} \in [\mathcal{J}]$ with $G = \tilde{\kappa} \circ \kappa(G)$. This in particular holds for any $\kappa \in \mathcal{I}$. Hence, $\mathcal{J}$ is a reversion of $\mathcal{I}$.

4. Suppose that $\mathcal{I}$ and $\mathcal{J}$ are orthogonal and let $H \in \sigma^{\mathcal{I}}(G) \cap \sigma^{\mathcal{J}}(G)$. Then we find $\kappa \in [\mathcal{I}]$, $\tilde{\kappa} \in [\mathcal{J}]$ with $\kappa(G) = \tilde{\kappa}(G) = H$. By orthogonality this implies $H = G$. Conversely, suppose $\sigma^{\mathcal{I}}(G) \cap \sigma^{\mathcal{J}}(G) = \{G\}$, and let $\kappa(G) = \tilde{\kappa}(G) =: H$ for some $\kappa \in [\mathcal{I}]$ and $\tilde{\kappa} \in [\mathcal{J}]$. Then $H \in \sigma^{\mathcal{I}}(G) \cap \sigma^{\mathcal{J}}(G)$, so $H = G$. Thus $\mathcal{I}$ and $\mathcal{J}$ are orthogonal.

5. $G \in \mathcal{G}$ can be transformed into an arbitrary $\tilde{G} \in \mathcal{G}$ by i) deleting the nodes in $\mathcal{V}_G \setminus \mathcal{V}_{\tilde{G}}$, ii) deleting all remaining edges from the set $\mathcal{E}_G \setminus \mathcal{E}_{\tilde{G}}$, iii) adding the nodes from $\mathcal{V}_{\tilde{G}} \setminus \mathcal{V}_G$ to G, iv) and adding the edges from $\mathcal{E}_{\tilde{G}} \setminus \mathcal{E}_G$.

□

4. Network Acceptance Sets - An Axiomatic System

In this section we collect *axioms* which we believe are minimal requirements on any reasonable acceptance set $\mathcal{A} \subset \mathcal{G}$ managing risk and resilience of (cyber) networks. We also discuss further properties of acceptance sets which may be desirable.

4.1. Acceptability and Means to Achieve Acceptability

First, we give introduce a universal axiom in the sense that it is not designed specifically for managing cyber risks, but it takes care of the interplay between acceptability and means to become acceptable. To this end we identify sets of basic network interventions from the previous section which lead to an improvement of some current configuration.

Definition 4.1. *Let $\mathcal{A} \subset \mathcal{G}$ and further let $\mathcal{I}$ be a set of network interventions.*

1. *$\mathcal{A}$ is said to be closed under $\mathcal{I}$ if $\sigma^{\mathcal{I}}(G) \subset \mathcal{A}$ for all $G \in \mathcal{A}$. In that case $\mathcal{I}$ is called **risk-reducing** for $\mathcal{A}$. A network intervention κ is called risk-reducing for $\mathcal{A}$ if the intervention set $\{\kappa\}$ is risk-reducing for $\mathcal{A}$.*

2. *$\mathcal{I}$ is **risk-increasing** for $\mathcal{A}$ if $\mathcal{G} \setminus \mathcal{A}$ is closed under $\mathcal{I}$, that is $\mathcal{I}$ is risk-reducing for $\mathcal{G} \setminus \mathcal{A}$.*

We now state the fundamental axiom of our risk management approach:

Axiom 1 *There is a set $\mathcal{I}^{\downarrow}$ of interventions such that* id $\subsetneq \mathcal{I}^{\downarrow}$ *and $\mathcal{I}^{\downarrow}$ is risk-reducing for $\mathcal{A}$.*

Remark 4.2. *1. The set $\mathcal{I}^{\downarrow}$ of risk-reducing interventions for $\mathcal{A}$ is interpreted as a set of means to potentially achieve acceptability for some unacceptable $G \in \mathcal{G} \setminus \mathcal{A}$. Therefore, a minimal condition on $\mathcal{I}^{\downarrow}$ is that $\mathcal{I}^{\downarrow} \setminus \{\text{id}\}$ should be non-empty. Moreover, for convenience we assume that* id *is contained in $\mathcal{I}^{\downarrow}$.*

2. *Note that we do not require $\mathcal{I}^{\downarrow}$ to contain all interventions which reduce the risk with respect to $\mathcal{A}$. For instance, drastic interventions like node splittings may reduce the risk but are possibly not available or not legitimate, at least not for every node, see the discussion on admissibility in Remark 6.3. Therefore, we also do not require conditions such as $\sigma^{\mathcal{I}^{\downarrow}}(G) \cap \mathcal{A} \neq \emptyset$ for all networks $G \in \mathcal{G}$ since there might be networks for which we do not have the means to transform them into an acceptable state.*

3. *Note that an implicit conclusion which could be drawn from Axiom 1, already mentioned in 1., is that the risk manager only chooses $\mathcal{I}^{\downarrow}$-strategies to secure some given network. One may, however, think of situations where strategies which combine risk-increasing and risk-reducing interventions also lead to acceptability. We do not explicitly exclude such strategies, see the discussion in Remark 6.2.*

4. *Moreover, note that we may view Axiom 1 as a monotonicity property of $\mathcal{A}$ with respect to the ordering $\preccurlyeq_{I^{\downarrow}}$ given in Proposition 3.9. Then $G \in \mathcal{A}$ and $G \preccurlyeq_{I^{\downarrow}} \tilde{G}$ imply $\tilde{G} \in \mathcal{A}$.*

Axiom 1 is essential to any risk management based on topological network interventions. This principle should also apply to risk measures for other types of networks of critical infrastructure mentioned in the introduction such as power or transportation networks.

Definition 4.3. *A non-empty set $\mathcal{A} \subseteq \mathcal{G}$ satisfying Axiom 1 is called a* ***network acceptance set****.*

4.2. Axioms for Resilience to Cyber Contagion

The following axioms are tailored to the management of pandemic (cyber) risks. First we combine two basic principles, namely that acceptable network configurations should exist, i.e. $\mathcal{A} \neq \emptyset$, and that the edgeless graphs $(\mathcal{V}, \emptyset)$, $\mathcal{V} \subset \mathbb{V}$, should be acceptable due to the absence of contagion channels:[6]

Axiom 2 *Every edgeless graph $(\mathcal{V}, \emptyset)$, $\mathcal{V} \subset \mathbb{V}$, of size $|\mathcal{V}| \geq 2$ is acceptable.*

In view of the functionality of a system, interconnectedness should be acceptable up to a certain degree. However, every network connection constitutes a possible channel of contagious transmission. Hence, there is a trade-off between functionality and risk in the sense of system vulnerability due to interconnectedness which is addressed in the following Axioms 3 and 4. First, as regards functionality, we require acceptability of some strongly connected networks. However, we add a size restriction to this requirement, since with increasing number of nodes, maintaining functionality while controlling the risk, is more feasible, see also Remark 4.6.

Axiom 3 *There is an $N_0 \in \mathbb{N}$ such that for all $N \geq N_0$ the acceptance set $\mathcal{A}$ contains a strongly connected network with N nodes.*

Next we address system vulnerability by specifying worst-case arrangements of networks that exceed any reasonable limit of risk.

[6] Note that if $|\mathcal{V}| = 1$, the edgeless graph of size 1 is also a star graph and complete. In order to be consistent with later axioms which in particular exclude complete graphs (Axiom 4 and 4') we choose here *not* to include graphs of size 1 in $\mathcal{A}$. Indeed note that the infection of the single node $v \in \mathcal{V} = \{v\}$ means that the full system is infected which is worst case from a pandemic point of view.

Definition 4.4. *Consider a network $G \in \mathcal{G}$ and a node $v^* \in \mathcal{V}_G$.*

1. *We call v^* a **super-spreader** if $\mathcal{N}_{v^*}^{G,out} = \mathcal{V}_G \setminus \{v^*\}$.*
2. *If, moreover, $\mathcal{N}_{v^*}^{G,in} = \mathcal{N}_{v^*}^{G,out} = \mathcal{V}_G \setminus \{v^*\}$, then v^* is called a **star node**.*

A cyber attack on a super-spreader may easily spread to significant parts or even the entire network. If, moreover, the network contains a star node v^*, which can be reached from any other node, an attack on an *arbitrary* part of the network always harbors the risk of spreading to the star and infecting large parts or the entire system from there. In our view, the presence of a star node constitutes, in any case, an unacceptable level of risk. In particular, this excludes any *complete graph* $G^c = (\mathcal{V}_{G^c}, (\mathcal{V}_{G^c} \times \mathcal{V}_{G^c}) \cap \mathbb{E})$, where each node is a star node.

Figure 3: A star graph (left), and a complete graph (right), consisting of $N = 8$ nodes. Both configurations are not acceptable according to Axiom 4 and 4'.

The strongest version of the following axiom is obtained when indeed all networks with super-spreaders (and thus in particular any network containing a star node) are excluded from the acceptance set, which seems sensible, at least if a targeted attack on the super-spreader is possible.

Axiom 4 *$\mathcal{A}$ does not contain any network with a super-spreader.*

However, this requirement may be too restrictive in the case of very large networks, if we also take into consideration the distribution of an initial infection. Suppose, for simplicity, that initially one uniformly chosen node is infected, and consider the *directed star graph* $G^* = (\mathcal{V}_{G^*}, \mathcal{E}_{G^*})$ with star node v^* where $\emptyset \neq \mathcal{V}_{G^*} \subset \mathbb{V}$ and

$$\mathcal{E}_{G^*} = \{(v^*, w) \mid w \in \mathcal{V}_{G^*} \setminus \{v^*\}\}.$$

For small network sizes, this is a highly vulnerable configuration. However, with increasing network size, the probability of an initial attack on v^* decreases. In the event that some node different from v^* is initially attacked, the infection cannot spread further in the network as in this example v^* is the only node with outgoing edges. Therefore, in the limit for large numbers of nodes, the system behavior of the directed star graph approaches that of the edgeless graph which is acceptable. Anyhow, if a network with super-spreader is indeed to be classified as acceptable, then this should only be allowed above a network size for which there already exist strongly connected configurations which are classified as acceptable. This line of reasoning leads to the following relaxed version of Axiom 4:

Axiom 4' *$\mathcal{A}$ does not contain any network with a star node. If there is an acceptable network with a super-spreader, then $\mathcal{A}$ also contains a strongly connected network of smaller size.*

Figure 4: A directed star graph (left), and a second graph that contains a super-spreader node (right), both consisting of $N = 8$ nodes.

Definition 4.5. *We call a non-empty set $\mathcal{A} \subset \mathcal{G}$ a* ***network acceptance set for pandemic cyber contagion*** *if it satisfies Axioms 1-3, and at least Axiom 4'.*

Remark 4.6. *Regarding the size restriction in Axiom 3, both Axioms 3 and 4 (or 4') can only be satisfied simultaneously if $N_0 > 2$ since for smaller network sizes a strongly connected configuration already corresponds to the complete graph. Alternatively, to avoid the contradiction, we could in principle have applied the size restriction to Axiom 4 instead of 3. However, the approach we have chosen is motivated by the fact that initial infections in a small network already affect a significant proportion of the overall system per se, and the presence of a few network edges are in principle sufficient for a shock to propagate through the entire system.*[7] *In practical applications, we should indeed expect to be confronted with networks of significantly larger sizes, and with increasing number of nodes, observing strongly connected graphs which do not contain super-spreaders or star nodes becomes more likely. Therefore, the requirement that $\mathcal{A}$ satisfies the Axioms 3 and 4 simultaneously is consistent with a tendency to favor* large networks *with a* diversified connectivity structure.

Further properties of the acceptance set may be reasonable. For example, suppose that the network G may be decomposed into k disconnected components $G_1, \ldots, G_k$. In that case, contagious risks can only spread within the components G_i of G but not between them. Therefore, the acceptability of all components may be seen as a sufficient condition for the acceptability of the full network:

Axiom 5 *$\mathcal{A}$ is closed under disjoint graph unions, i.e., if $G, H \in \mathcal{A}$ with $\mathcal{V}_G \cap \mathcal{V}_H = \emptyset$, then $G \cup H := (\mathcal{V}_G \cup \mathcal{V}_H, \mathcal{E}_G \cup \mathcal{E}_H) \in \mathcal{A}$.*

If we do not endow the single nodes $v \in \mathcal{V}_G$ of a network G with a particular meaning, one might identify networks which are isomorphic and thus require that:

[7]Note also that this is consistent with our requirement in Axiom 1 to exclude all networks of size 1 from the acceptance set.

Axiom 6 *Topological invariance: $\mathcal{A}$ is closed under graph isomorphisms, i.e., for any two networks $G, \tilde{G} \in \mathcal{G}$ which are isomorphic we have $G \in \mathcal{A}$ if and only if $\tilde{G} \in \mathcal{A}$.*

This property resembles the concept of distribution-invariant risk measures common in financial economics. Indeed, if graphs are isomorphic, then their degree distributions coincide. However, note that in situations where the network components resemble particular entities, some of which may need to be prioritized in terms of protection, f.e., entities that belong to critical infrastructures, topological invariance is not appropriate.

5. Cost Functions

The final ingredient to our risk management framework is the cost function representing some type of price we pay for altering a given network. The cost function measures the consequences of the supervisors decisions and potentially quantifies the resources needed to achieve acceptability.

Definition 5.1. *Given a network acceptance set $\mathcal{A} \subset \mathcal{G}$ and a set of interventions $\mathcal{I}^{\downarrow}$ which together satisfy Axiom 1, a map $\mathcal{C} : \mathcal{G} \times \mathcal{G} \to \mathbb{R} \cup \{\infty\}$ with*

C1 $\mathcal{C}(G, G) = 0$ for all $G \in \mathcal{G}$

C2 $\mathcal{C}(G, H) \geq 0$ whenever $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$

is called a cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$.

The following two types of cost functions appear naturally:

1. A quantification of the *monetary* cost of transforming a graph G into $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$, see Section 5.1.

2. A quantification of the cost of transforming a graph G into $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$ in terms of the corresponding *impact on network functionality*, see Section 5.2.

Other potentially useful or desirable properties of a cost function are as follows:

C3 Every non-trivial network intervention comes at a real cost, i.e.,

$$\mathcal{C}(G, H) = 0 \Rightarrow G = H \text{ for all } H, G \in \mathcal{G}.$$

C4 It might also be reasonable to require that the absolute cost of a direct transformation of G to H should not be more expensive than first transforming to an intermediate configuration M, i.e., for all $G, H, M \in \mathcal{G}$ such that $M \in \sigma^{\mathcal{I}^{\downarrow}}(G)$, and $H \in \sigma^{\mathcal{I}^{\downarrow}}(M)$ we have

$$\mathcal{C}(G, H) \leq \mathcal{C}(G, M) + \mathcal{C}(M, H).$$

Moreover, assume that there is also a fixed set $\mathcal{I}^{\uparrow}$ of risk-increasing interventions for $\mathcal{A}$ (recall Definition 4.1).

C5 In case $\mathcal{I}^{\downarrow} \perp \mathcal{I}^{\uparrow}$, it may be plausible to assume that risk-increasing interventions come with negative costs, i.e.,

$$\mathcal{C}(G, H) \leq 0 \text{ if } H \in \sigma^{\mathcal{I}^{\uparrow}}(G).$$

This property is particularly reasonable if costs are measured in terms of network functionality. However, it might not be suitable in case of a monetary cost function where every network manipulation, also the bad ones, is associated with some (non-negative) expense.

C6 *If $\mathcal{I}^{\downarrow} \perp \mathcal{I}^{\uparrow}$ and $\mathcal{I}^{\downarrow} \triangle \mathcal{I}^{\uparrow}$, an even stronger tightening of the previous property is to assume that $\mathcal{C}$ satisfies*

$$\mathcal{C}(G,H) = -\mathcal{C}(H,G) \text{ for all } H \in \sigma^{\mathcal{I}^{\downarrow}}(G) \cup \sigma^{\mathcal{I}^{\uparrow}}(G) \text{ and } G \in \mathcal{G}.$$

5.1. Examples of Monetary Cost Functions

Consider any network acceptance set $\mathcal{A} \subset \mathcal{G}$ and a set of interventions $\mathcal{I}^{\downarrow}$ which together satisfy Axiom 1. A way to construct a monetary cost function based on the cost of any basic intervention $\kappa \in \mathcal{I}^{\downarrow}$ is the following: Suppose we associate an initial cost $\tilde{p}(\kappa) \in [0,\infty)$ with each $\kappa \in \mathcal{I}^{\downarrow}$ such that $\tilde{p}(\mathrm{id}) = 0$, and for any $\mathcal{I}^{\downarrow}$-strategy κ set

$$p(\kappa) := \inf\left\{\sum_{i=1}^{n} \tilde{p}(\kappa_i) \mid \kappa = \kappa_n \circ \cdots \circ \kappa_1, \kappa_i \in \mathcal{I}^{\downarrow}, i = 1,\ldots,n, n \in \mathbb{N}\right\}. \tag{2}$$

Then consider the minimal total cost for the transformation of G into H:

$$\mathcal{C}(G,H) := \inf\{p(\kappa) \mid \kappa \in [\mathcal{I}^{\downarrow}], \kappa(G) = H\}, \quad \inf\emptyset := \infty. \tag{3}$$

Note that p conincides with $\tilde{p}$ on $\mathcal{I}^{\downarrow}$ if and only if $\tilde{p}$ is *consistent*, that is if $\kappa \in \mathcal{I}^{\downarrow}$ satisfies $\kappa = \kappa_n \circ \cdots \circ \kappa_1$ for some interventions $\kappa_i \in \mathcal{I}^{\downarrow}$, $i = 1,\ldots,n$, $n \in \mathbb{N}$, we must have $\tilde{p}(\kappa) = \sum_{i=1}^{n} \tilde{p}(\kappa_i)$. Of course, consistency of $\tilde{p}$ on $\mathcal{I}^{\downarrow}$ is automatically satisfied in case that $\kappa = \kappa_n \circ \cdots \circ \kappa_1$ for some $\kappa, \kappa_1, \ldots, \kappa_n \in \mathcal{I}^{\downarrow}$ implies that $\kappa_j = \kappa$ for some $j \in \{1,\ldots,n\}$ and $\kappa_i = \mathrm{id}$ for all $i \neq j$. The following lemma is easily verified.

Lemma 5.2. *p is subadditive in the sense that for all $\kappa, \alpha \in [\mathcal{I}^{\downarrow}]$ we have $p(\kappa \circ \alpha) \leq p(\kappa) + p(\alpha)$.*

Proposition 5.3. *Suppose that $\mathcal{C}$ is given by* (3)*. Then:*

1. *$\mathcal{C}(G,H) < \infty$ if and only if $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$.*
2. *$\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$ which satisfies C4.*
3. *Further suppose that $\inf\{\tilde{p}(\kappa) \mid \kappa \in \mathcal{I}^{\downarrow} \setminus \{\mathrm{id}\}\} > 0$, then C3 is satisfied.*
4. *Moreover, if $\mathcal{I}^{\downarrow}$ is finite and $\tilde{p}(\kappa) > 0$ for all $\kappa \in \mathcal{I}^{\downarrow}$ such that $\kappa \neq \mathrm{id}$, then the infimum in* (3) *is attained whenever $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$. In other words, if $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$, then there are optimal $\mathcal{I}^{\downarrow}$-strategies κ for transforming G into H in the sense that $\kappa(G) = H$ and $p(\kappa) = \mathcal{C}(G,H)$.*

Proof. 1. is obvious.
2. $\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$ which satisfies *C4*: *C1* follows from $p(\mathrm{id}) = 0$, whereas *C2* is implied by $\tilde{p}(\kappa) \geq 0$ for each $\kappa \in \mathcal{I}^{\downarrow}$. As for *C4* consider $G, M, H \in \mathcal{G}$ and suppose that there is $\kappa, \alpha \in [\mathcal{I}^{\downarrow}]$ with $\alpha(G) = M$ and $\kappa(M) = H$. Then $\kappa \circ \alpha(G) = H$, and by Lemma 5.2 above we have that $\mathcal{C}(G,H) \leq \mathcal{C}(G,M) + \mathcal{C}(M,H)$.
3. Clearly, if $\nu := \inf\{p(\kappa) \mid \kappa \in \mathcal{I}^{\downarrow} \setminus \{\mathrm{id}\}\} > 0$, then $p(\kappa) > \nu$ for all $\kappa \in [\mathcal{I}^{\downarrow}]$ such that $\kappa \neq \mathrm{id}$. Hence, $\mathcal{C}(G,H) = 0$ is only possible if $H = G$.
4. In order to show that there are optimal $\mathcal{I}^{\downarrow}$-strategies in case $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$, pick any $\kappa \in [\mathcal{I}^{\downarrow}]$ such that $\kappa(G) = H$. Note that $\nu = \min\{\tilde{p}(\kappa) \mid \kappa \in \mathcal{I}^{\downarrow} \setminus \{\mathrm{id}\}\} > 0$, and let $m \in \mathbb{N}$ be such that $m\nu > p(\kappa)$. Denote by $[\mathcal{I}^{\downarrow}]_m$ the set of all $\mathcal{I}^{\downarrow}$-strategies which allow for a decomposition $\alpha = \alpha_k \circ \ldots \alpha_1$ where $\alpha_1, \ldots, \alpha_k \in \mathcal{I}^{\downarrow}$ and $k \leq m$. Note that $p(\alpha) \geq m\nu > p(\kappa)$ for all $\alpha \in [\mathcal{I}^{\downarrow}] \setminus [\mathcal{I}^{\downarrow}]_m$. Therefore, it follows that

$$\mathcal{C}(G,H) = \inf\{p(\alpha) \mid \alpha \in [\mathcal{I}^{\downarrow}]_m, \alpha(G) = H\}.$$

Now the assertion follows from $[\mathcal{I}^{\downarrow}] \setminus [\mathcal{I}^{\downarrow}]_m$ being a finite set. □

Note that the properties *C5* and *C6* do not apply for monetary costs given by (3). Suppose that there is also a set $\mathcal{I}^{\uparrow}$ of risk-increasing interventions for $\mathcal{A}$. $\mathcal{I}^{\uparrow}$ may not be desirable from a risk perspective, but may, for instance, increase the functionality of the network. Therefore, one could associate any $\kappa \in \mathcal{I}^{\uparrow}$ with a revenue which is represented by a negative price. Basing costs on the price of interventions in $\mathcal{I}^{\downarrow}$ we obtain the following cost function

$$\mathcal{C}(G,H) := \begin{cases} \inf\{p(\kappa) \mid \kappa \in [\mathcal{I}^{\downarrow}], \kappa(G) = H\} & \text{if } H \in \sigma^{\mathcal{I}^{\downarrow}}(G) \\ -\mathcal{C}(H,G) & \text{if } H \in \sigma^{\mathcal{I}^{\uparrow}}(G) \\ \infty & \text{else.} \end{cases} \tag{4}$$

Proposition 5.4. *Suppose that* p *is consistent on* $\mathcal{I}^{\downarrow}$. *Further suppose that* $\mathcal{I}^{\downarrow} \perp \mathcal{I}^{\uparrow}$ *and* $\mathcal{I}^{\downarrow} \triangle \mathcal{I}^{\uparrow}$, *and that* $\mathcal{C}$ *is given by* (4). *Then:*

1. $\mathcal{C}$ *is well-defined.*
2. $\mathcal{C}(G,H) < \infty$ *if and only if* $H \in \sigma^{\mathcal{I}^{\downarrow}}(G) \cup \sigma^{\mathcal{I}^{\uparrow}}(G)$.
3. $\mathcal{C}$ *is a cost function for* $(\mathcal{A}, \mathcal{I}^{\downarrow})$ *which satisfies C4–C6.*
4. *Further suppose that* $\inf\{\tilde{p}(\kappa) \mid \kappa \in \mathcal{I}^{\downarrow} \setminus \{\mathrm{id}\}\} > 0$, *then C3 is satisfied.*
5. *If* $\mathcal{I}^{\downarrow}$ *is finite and* $\tilde{p}(\kappa) > 0$ *for all* $\kappa \in \mathcal{I}^{\downarrow}$ *such that* $\kappa \neq \mathrm{id}$, *then for every* $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$ *there are optimal* $\mathcal{I}^{\downarrow}$*-strategies* κ *for transforming* G *into* H *in the sense that* $\kappa(G) = H$ *and* $p(\kappa) = \mathcal{C}(G,H)$.

Proof. By Proposition 3.9 we have $\sigma^{\mathcal{I}^{\downarrow}}(G) \cap \sigma^{\mathcal{I}^{\uparrow}}(G) = \{G\}$, and $H \in \sigma^{\mathcal{I}^{\uparrow}}(G)$ if and only if $G \in \sigma^{\mathcal{I}^{\downarrow}}(H)$. It follows that $\mathcal{C}$ is well-defined. By definition $\mathcal{C}$ satisfies $\mathcal{C}(G,H) < \infty$ if and only if $H \in \sigma^{\mathcal{I}^{\downarrow}}(G) \cup \sigma^{\mathcal{I}^{\uparrow}}(G)$, and we also have *C5* and *C6*. The other properties follow as in the proof of Proposition 5.3. □

Another way to include revenues for applying interventions from $\mathcal{I}^{\uparrow}$ is to define $\tilde{p}$ not only on $\mathcal{I}^{\downarrow}$ as above but also on $\mathcal{I}^{\uparrow}$, where $\tilde{p}(\kappa) \in (-\infty, 0]$ for all $\kappa \in \mathcal{I}^{\uparrow} \setminus \{\mathrm{id}\}$. Then let p be given as in (2) on $[\mathcal{I}^{\downarrow}]$ and by

$$p(\kappa) := \sup\left\{\sum_{i=1}^{n} \tilde{p}(\kappa_i) \mid \kappa = \kappa_n \circ \cdots \circ \kappa_1, \kappa_i \in \mathcal{I}^{\uparrow}, i = 1, \ldots, n, n \in \mathbb{N}\right\}. \tag{5}$$

for $\kappa \in [\mathcal{I}^{\uparrow}]$. Note that taking the supremum in (5) means that we require that the $\mathcal{I}^{\uparrow}$-strategy κ yields a revenue no matter from which perspective we look at κ. Again, one easily verifies that

Lemma 5.5. p *is subadditive on* $\mathcal{I}^{\downarrow}$ *and superadditive on* $\mathcal{I}^{\uparrow}$ *in the sense that for all* $\kappa, \alpha \in [\mathcal{I}^{\uparrow}]$ *we have* $p(\kappa \circ \alpha) \geq p(\kappa) + p(\alpha)$.

Now consider the following monetary cost function

$$\mathcal{C}(G,H) := \begin{cases} \inf\{p(\kappa) \mid \kappa \in [\mathcal{I}^{\downarrow}], \kappa(G) = H\} & \text{if } H \in \sigma^{\mathcal{I}^{\downarrow}}(G) \\ \sup\{p(\kappa) \mid \kappa \in [\mathcal{I}^{\uparrow}], \kappa(G) = H\} & \text{if } H \in \sigma^{\mathcal{I}^{\uparrow}}(G) \\ \infty & \text{else.} \end{cases} \tag{6}$$

Proposition 5.6. *Suppose that* $\mathcal{I}^{\downarrow} \perp \mathcal{I}^{\uparrow}$, *and that* $\mathcal{C}$ *is given by* (6). *Then:*

1. $\mathcal{C}$ *is well-defined.*
2. $\mathcal{C}(G,H) < \infty$ *if and only if* $H \in \sigma^{\mathcal{I}^{\downarrow}}(G) \cup \sigma^{\mathcal{I}^{\uparrow}}(G)$.

3. *$\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$ which satisfies C4–C5.*

4. *Further suppose that* $\inf\{|\tilde{p}(\kappa)| \mid \kappa \in (\mathcal{I}^{\downarrow} \cup \mathcal{I}^{\uparrow}) \setminus \{\mathrm{id}\}\} > 0$*, then C3 is satisfied.*

5. *If $\mathcal{I}^{\downarrow}$ is finite and $\tilde{p}(\kappa) > 0$ for all $\kappa \in \mathcal{I}^{\downarrow}$ such that $\kappa \neq \mathrm{id}$, then for every $H \in \sigma^{\mathcal{I}^{\downarrow}}(G)$ there are optimal $\mathcal{I}^{\downarrow}$-strategies κ or transforming G into H in the sense that such that $\kappa(G) = H$ and $p(\kappa) = \mathcal{C}(G, H)$.*

6. *If $\mathcal{I}^{\uparrow}$ is finite and $\tilde{p}(\kappa) < 0$ for all $\kappa \in \mathcal{I}^{\uparrow}$ such that $\kappa \neq \mathrm{id}$, then for every $H \in \sigma^{\mathcal{I}^{\uparrow}}(G)$ there is $\kappa \in [\mathcal{I}^{\uparrow}]$ such that $\kappa(G) = H$ and $p(\kappa) = \mathcal{C}(G, H)$.*

Proof. The proof follows by similar arguments as in the proof of Proposition 5.4. $\square$

Note that in the situation of Proposition 5.6, *C6* is only satisfied under strong (trivializing) assumptions on $\mathcal{I}^{\downarrow}$, $\mathcal{I}^{\uparrow}$, and p. In that case the cost functions (4) and (6) coincide. Also note another issue with the cost functions given in (4) or (6): Suppose that $H \in \sigma^{\mathcal{I}^{\uparrow}}(G)$ and $M \in \sigma^{\mathcal{I}^{\downarrow}}(H)$, then it may for instance be that $M \notin \sigma^{\mathcal{I}^{\downarrow}}(G) \cup \sigma^{\mathcal{I}^{\uparrow}}(G)$ and hence $\mathcal{C}(G, M) = \infty$ even though $\mathcal{C}(G, H) < \infty$ and $\mathcal{C}(H, M) < \infty$. As $\mathcal{C}(G, H) + \mathcal{C}(H, M) < \infty$, which could be seen as the cost of first transforming G into H and then into M, it may seem awkward that $\mathcal{C}(G, M) = \infty$. Such issues may be overcome, and one could think of conditions ensuring subadditivity in the sense that always $\mathcal{C}(G, M) \leq \mathcal{C}(G, H) + \mathcal{C}(H, M)$ which would constitute a strengthening of *C4*. This is, however, not in the scope of this paper, and left for future research.

5.2. Examples of Cost Functions based on Loss of Network Functionality

Let $\mathcal{A}$ satisfy Axiom 1 with $\mathcal{I}^{\downarrow}$. A natural choice for the cost $\mathcal{C}$ is a function that quantifies the difference in functionality $\mathcal{F} : \mathcal{G} \to \mathbb{R}$ between two networks such as

$$\mathcal{C}(G, H) = h(\mathcal{F}(G) - \mathcal{F}(H)) \tag{7}$$

with some suitable $h : \mathbb{R} \to \mathbb{R}$. Note that the Properties *C1*, *C4*, and *C6* solely depend on the choice of h, and one easily verifies the follow result:

Lemma 5.7. *Consider a cost function of type* (7)*. Then*

1. *Property C1 is satisfied if and only if $h(0) = 0$.*

2. *If h is sub-additive, then C4 holds.*

3. *C6 holds if h may be chosen to be anti-symmetric, i.e., $h(x) = -h(-x)$ for all $x \in \mathbb{R}$.*

Network functionality is typically measured by considering the average node distance within the network: A smaller average value corresponds to a faster or more efficient data flow. There are two common concepts to define the distance between nodes:

- *Shortest path length:* Given two nodes v and w in a network G, we denote by l_{vw}^{G} the length of a path from node v to w that passes through a minimum number of edges. If there is no path from v to w, then we set $l_{vw}^{G} = \min \emptyset := \infty$.

- *Communicability:* An alternative concept[8] is given by the *communicability* $\mathfrak{c}_{v_i v_j}^{G}$ between nodes v_i and v_j in a graph G of size N with enumerated vertices $v_1, \ldots, v_N$, defined as the (i, j)th entry of the matrix exponential e^{A_G} of the adjacency matrix A_G, i.e.

$$\mathfrak{c}_{v_i v_j}^{G} := \sum_{k=0}^{\infty} \frac{(A_G^k)(i,j)}{k!} = e^{A_G}(i,j), \text{ where } e^{A_G} := I_N + A_G + \frac{A_G^2}{2!} + \frac{A_G^3}{3!} + \cdots = \sum_{k=0}^{\infty} \frac{A_G^k}{k!}$$

[8] By some authors, it has been emphasized that the analysis of shortest paths only provides an incomplete picture of the full system since the flow of information, data, or goods in a network may take place through many different routes, see the discussion in [29] for example.

and I_N is the identity matrix in $\mathbb{R}^{N\times N}$. Note that $A_G^k(i,j)$ gives the number of walks of length k from node v_i to v_j, and therefore $\mathfrak{c}_{v_iv_j}^G$ is a weighted sum of all walks from v_i to v_j, where walks of length k are penalized by a factor of $1/k!$.

5.2.1. Functionality Based on Shortest Paths

A canonical choice for a global measure of network functionality based on shortest paths is given by the *graph efficiency* as defined in [52], which takes the average over all the reverse distances in a graph:

$$\mathcal{F}(G) = \frac{1}{|\mathcal{V}_G|(|\mathcal{V}_G|-1)} \sum_{v,w,v\neq w} \frac{1}{l_{vw}^G} \qquad \Big(\frac{1}{\infty} := 0\Big). \tag{8}$$

Lemma 5.8. *Suppose that $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^\downarrow \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso}$. Then $\mathcal{C}$ given by* (7) *and* (8) *and a strictly increasing function h with $h(0)=0$ is a cost function for $(\mathcal{A},\mathcal{I}^\downarrow)$ which satisfies the following constrained version of C3:*

$$\forall G \in \mathcal{G}\, \forall H \in \sigma^{\mathcal{I}^\downarrow}(G): \quad \mathcal{C}(G,H) = 0 \Rightarrow G = H. \tag{9}$$

Moreover, C5 holds for any choice of $\mathcal{I}^\uparrow \subset \mathcal{I}_{e\_add}$.

Proof. C1 follows from $h(0)=0$. In order to prove *C2* and (9) we show that $\mathcal{F}(G)$ is non-increasing whenever we apply a intervention in $\mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso}$ to G and even strictly decreasing if the intervention alters G. As a consequence, for all $\kappa \in [\mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso}]$ and thus for all $\kappa \in [\mathcal{I}^\downarrow]$ we obtain that $\mathcal{F}(\kappa(G)) \leq \mathcal{F}(G)$ which implies $h(\mathcal{F}(G) - \mathcal{F}(\kappa(G))) \geq h(0) = 0$ showing *C2*, and $\mathcal{F}(\kappa(G)) < \mathcal{F}(G)$ in case $\kappa(G) \neq G$ implying $h(\mathcal{F}(G) - \mathcal{F}(\kappa(G))) > h(0) = 0$ which is (9).

Let us first consider edge deletions: Fix $G \in \mathcal{G}$ and delete an edge $(q,r) \in \mathbb{E}$. Let $\tilde{G} := \kappa_{e\_del}^{(q,r)}(G)$. The deletion of the edge (q,r) does not create any new paths and therefore $l_{vw}^G \leq l_{vw}^{\tilde{G}}$ for all nodes $v,w \in \mathcal{V}_G$. Moreover, if $(q,r) \in \mathcal{E}_G$, then we necessarily have $l_{qr}^G < l_{qr}^{\tilde{G}}$, i.e., there is at least one node pair where the inequality is strict. We thus obtain $\mathcal{F}(\tilde{G}) \leq \mathcal{F}(G)$ for all networks $G \in \mathcal{G}$ and $(q,r) \in \mathbb{E}$, and "=" holds exactly when we have $(q,r) \notin \mathcal{E}_G$, i.e., if and only if $\tilde{G} = G$.

Note that the isolation of a subgraph, that is $\tilde{G} := \kappa_{iso}^{\mathcal{W}}(G)$ where $\mathcal{W} \subset \mathbb{V}$, is a sequence of edge deletions, namely deleting all edges connecting nodes in $\mathcal{V}_G \setminus \mathcal{W}$ with some node in $\mathcal{W}$. Hence, also in this case we obtain $\mathcal{F}(\tilde{G}) \leq \mathcal{F}(G)$, and "=" holds exactly when $v \notin \mathcal{V}_G$ for all $v \in \mathcal{W}$ or when the subgraph given by the nodes $\mathcal{W} \cap \mathcal{V}_G$ is already in G, i.e., if and only if $\tilde{G} = G$.

Recalling Proposition 3.9, *C5* now follows from $\mathcal{I}_{e\_add} \perp (\mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso})$, $\mathcal{I}_{e\_add} \triangle \mathcal{I}_{e\_add}$, and the first part of the proof which then shows that $\mathcal{F}(H) \geq \mathcal{F}(G)$ whenever $H \in \sigma^{\mathcal{I}_{e\_add}}(G)$, since the latter is equivalent to $G \in \sigma^{\mathcal{I}_{e\_del}}(H)$. □

However, measuring network functionality in terms of shortest paths may come with some difficulties when allowing for $\mathcal{I}_{\mathrm{n}\_split} \subseteq \mathcal{I}^\downarrow$ as is illustrated by the following example.

Example 5.9. *Let H be obtained from a network G of size N after the conduction of a node split. For $\mathcal{F}$ to be monotonically decreasing under this intervention, the shortest path lengths in H must satisfy*

$$\frac{N-1}{N+1} \sum_{v,w \in \mathcal{V}_H, v\neq w} \frac{1}{l_{vw}^H} \leq \sum_{v,w \in \mathcal{V}_G, v \neq w} \frac{1}{l_{vw}^G}. \tag{10}$$

Consider a graph $G = G_1 \cup G_2$ consisting of two isolated components G_1, G_2 where

- *G_1 is depicted in Figure 5,*
- *G_2 be a graph of $N-3$ isolated nodes (edgeless graph) such that $\mathcal{V}_{G_1} \cap \mathcal{V}_{G_2} = \emptyset$.*

Now assume that node $b \in \mathcal{V}_{G_1}$ is split as depicted in Figure 5. Let the resulting transformation of component G_1 be denoted by H_1.

G_1 $\qquad$ H_1

Figure 5: Node b is splitted by adding node $\tilde{b} \notin \mathcal{V}_G$ to the network and replacing the edges in $\{(b,c),(c,b)\}$ by those from $\{(\tilde{b},c),(c,\tilde{b})\}$.

We obtain

$$\sum_{v,w \in \mathcal{V}_{H_1}, v \neq w} \frac{1}{l_{vw}^{H_1}} = 2 \cdot \Big(1 + 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{3} + 1\Big) = \sum_{v,w \in \mathcal{V}_{G_1}, v \neq w} \frac{1}{l_{vw}^{G_1}} + \frac{8}{3},$$

and since the components G_1 and G_2 are not connected by any path in the network G, we have

$$\sum_{v,w \in \mathcal{V}_{H}, v \neq w} \frac{1}{l_{vw}^{H}} = \sum_{v,w \in \mathcal{V}_{H_1}, v \neq w} \frac{1}{l_{vw}^{H_1}} \quad \text{and} \quad \sum_{v,w \in \mathcal{V}_{G}, v \neq w} \frac{1}{l_{vw}^{G}} = \sum_{v,w \in \mathcal{V}_{G_1}, v \neq w} \frac{1}{l_{vw}^{G_1}}.$$

Hence, (10) *becomes*

$$\frac{N-1}{N+1} \left(\sum_{v,w \in \mathcal{V}_{G}, v \neq w} \frac{1}{l_{vw}^{G}} + \frac{8}{3} \right) \leq \sum_{v,w \in \mathcal{V}_{G}, v \neq w} \frac{1}{l_{vw}^{G}}.$$

This latter inequality is violated whenever N is large enough, which can be achieved by blowing up the network component G_2. Therefore, in this case, if $h : \mathbb{R} \to \mathbb{R}$ is strictly increasing with $h(0) = 0$, we do not satisfy C2.

5.2.2. Functionality Based on Network Communicability

Taking the average over all the local communicabilities yields the global measure

$$\mathcal{F}(G) = \frac{1}{|\mathcal{V}_G|^2} \sum_{v,w} \mathfrak{c}_{vw}^G \tag{11}$$

for a network G. In contrast to shortest paths, it may be useful to include self-communicabilities, that are entities $\mathfrak{c}_{vv}$, into the consideration since walks of from a node to itself correspond to closed communication loops. Basing the cost function on communicability we do not only satisfy *C2* in case of edge deletions, but—in contrast to shortest path based costs—also when risk-reduction is achieved by node splitting.

Lemma 5.10. *Suppose that $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$. Then $\mathcal{C}$ given by* (7) *and* (11) *and a strictly increasing function h with $h(0) = 0$ is a cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$ which satisfies* (9)*. Moreover, C5 holds for any choice of $\mathcal{I}^{\uparrow} \subset \mathcal{I}_{e\_add} \cup \mathcal{I}_{merge}$.*

Proof. *C1* follows from $h(0) = 0$. As in the proof of Lemma 5.8 we prove *C2* and (9) by showing that $\mathcal{F}(G)$ is non-increasing whenever we apply a intervention in $\mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$ to G and even strictly decreasing if the intervention alters G.

Let $G \in \mathcal{G}$ with adjacency matrix A_G, given some enumeration of the nodes $\mathcal{V}_G$. Let us first consider edge deletions. To this end, let $\tilde{G} = \kappa_{e\_del}^{(v_i,v_j)}(G)$ where $v_i, v_j \in \mathcal{V}_G$. If $(v_i, v_j) \in \mathcal{E}_G$, then

$A_{\tilde{G}}(i,j) < A_G(i,j)$, and indeed $A^k_{\tilde{G}}(l,m) < A^k_G(l,m)$ for every $k \geq 1$ and l,m such that (v_i, v_j) is element of a walk of length k from v_l to v_m.[9] Hence, $\mathfrak{c}^{\tilde{G}}_{vw} < \mathfrak{c}^{G}_{vw}$ for all $v, w \in \mathcal{V}_G$ where (v_i, v_j) lies on a walk from v to w, yielding $\mathcal{F}(\tilde{G}) < \mathcal{F}(G)$. Therefore, we conclude that $\mathcal{F}(\tilde{G}) \leq \mathcal{F}(G)$ and $\mathcal{F}(\tilde{G}) = \mathcal{F}(G)$ if and only if $G = \tilde{G}$. Conversely, if $\tilde{G}$ is obtained by adding an edge to the network G, and thus G is obtained by an edge deletion in $\tilde{G}$, the previous arguments show that $\mathfrak{c}^{\tilde{G}}_{vw} > \mathfrak{c}^{G}_{vw}$, and thus $\mathcal{F}(\tilde{G}) > \mathcal{F}(G)$ unless $G = \tilde{G}$.

Next let us consider node splittings. If $\tilde{G}$ results from a node splitting intervention in G, then, conversely, G can be obtained by a node merging intervention in $\tilde{G}$. Therefore, it suffices to prove that $\mathcal{F}$ is increasing under node merging. So let $G = \kappa^{v_i,v_j}_{merge}(\tilde{G})$ be the graph obtained after merging two nodes $v_i, v_j \in \mathcal{V}_{\tilde{G}}$ in a network $\tilde{G}$ of size N. In case this merge operation is non-trivial, that is $G \neq \tilde{G}$, assuming $i < j$, this intervention can be described by a matrix operation on the adjacency matrix $A_{\tilde{G}}$, i.e., $A_G = \hat{M} \cdot A_{\tilde{G}} \cdot \hat{M}^T$ with $\hat{M} \in \{0,1\}^{(N-1)\times N}$ defined as

$$\hat{M}(l,m) = \begin{cases} 1, & \text{for } l = m < j \\ 1, & \text{for } l = i, m = j \\ 1, & \text{for } j \leq l \leq N-1, m = l+1 \\ 0, & \text{else.} \end{cases}$$

One verifies that the product $\hat{M}^T\hat{M}$ equals 1 on the diagonal. Let $I_N \in \mathbb{R}^{N\times N}$ denote the identity matrix. Then it follows that $\hat{M}^T\hat{M} \geq I_N$ in the sense that componentwise we have $(\hat{M}^T\hat{M})(l,m) \geq I_N(l,m)$ for all $l,m = 1,\ldots,N$. Since all entries in $A_{\tilde{G}}$ are non-negative we estimate

$$\begin{aligned} (A_G)^k &= \left(\hat{M} \cdot A_{\tilde{G}} \cdot \hat{M}^T\right)^k \\ &= \hat{M} \cdot A_{\tilde{G}} \cdot \hat{M}^T \cdot \hat{M} \cdot A_{\tilde{G}} \cdot \hat{M}^T \cdot \hat{M} \cdot A_{\tilde{G}} \cdots A_{\tilde{G}}\hat{M}^T \\ &\geq \hat{M} \cdot A_{\tilde{G}} \cdot I_N \cdot A_{\tilde{G}} \cdot I_N \cdot A_{\tilde{G}} \cdots A_{\tilde{G}}\hat{M}^T \\ &= \hat{M} \cdot (A_{\tilde{G}})^k \cdot \hat{M}^T. \end{aligned}$$

Thus we obtain

$$\sum_{l=1}^{N-1}\sum_{m=1}^{N-1}(A_G)^k(l,m) \geq \sum_{l=1}^{N-1}\sum_{m=1}^{N-1}(\hat{M}\cdot(A_{\tilde{G}})^k\cdot\hat{M}^T)(l,m) = \sum_{l=1}^{N}\sum_{m=1}^{N}(A_{\tilde{G}})^k(l,m)$$

for all $l,m = 1,\cdots,N$, and therefore[10]

$$\sum_{v_i,v_j\in\mathcal{V}_G}\mathfrak{c}^{G}_{v_iv_j} \geq \sum_{v_i,v_j\in\mathcal{V}_{\tilde{G}}}\mathfrak{c}^{\tilde{G}}_{v_iv_j}$$

for the sum of all communicabilities. Further, since $\tilde{G}$ is larger than G, this yields strict inequality when taking the average value, i.e., $\mathcal{F}(\tilde{G}) < \mathcal{F}(G)$. Therefore, we conclude that $\mathcal{F}(\tilde{G}) \leq \mathcal{F}(G)$ for all $\tilde{G}$ obtained by performing a node splitting on G, and $\mathcal{F}(\tilde{G}) = \mathcal{F}(G)$ if and only if $G = \tilde{G}$

[9] Note that the full argument can also be extended to the case of weighted networks for the reduction of edge weight $w(i,j)$ of the corresponding edge.

[10] Note that we find "$>$" if and only if there is a matrix entry (l,m) with $A_{\tilde{G}}\hat{M}^T\hat{M}A_{\tilde{G}}(l,m) > A_{\tilde{G}}I_NA_{\tilde{G}}(l,m)$, which means that

$$A_{\tilde{G}}\hat{M}^T\hat{M}A_{\tilde{G}}(l,m) = \sum_{p=1}^{N}\sum_{o=1}^{N}A_{\tilde{G}}(l,o)\hat{M}^T\hat{M}(o,p)A_{\tilde{G}}(p,m) > \sum_{o=1}^{N}A_{\tilde{G}}(l,o)A_{\tilde{G}}(o,m).$$

This is the case if and only if $A_{\tilde{G}}(l,i) > 0$ and $A_{\tilde{G}}(j,m) > 0$, or $A_{\tilde{G}}(l,j) > 0$ and $A_{\tilde{G}}(i,m) > 0$, which means that $\mathcal{N}^{\tilde{G},in}_{v_i}, \mathcal{N}^{\tilde{G},out}_{v_j} \neq \emptyset$, or $\mathcal{N}^{\tilde{G},out}_{v_i}, \mathcal{N}^{\tilde{G},in}_{v_j} \neq \emptyset$. In other words, a node split reduces some communicabilities in a network if and only if the split corresponds to an actual separation of contagion channels.

As regards *C5*, note that $(\mathcal{I}_{e\_del} \cup \mathcal{I}_{split}) \perp (\mathcal{I}_{e\_add} \cup \mathcal{I}_{merge})$. Moreover, we have already shown $\mathcal{F}(\kappa(G)) \geq \mathcal{F}(G)$ for any $\kappa \in \mathcal{I}_{e\_add} \cup \mathcal{I}_{merge}$.

$\square$

5.3. Costs under Partial Information

In order to determine the functionality of networks, information about a large part or even the entire network topology is usually required. For example, the network communicabilities $\mathfrak{c}_{vw}^{G}$ in (11) generally have to be calculated from all the entries of the adjacency matrix A_G. In practice, however, this information is often only available to a very limited extent, especially for large networks such as the internet. There are different ways to deal with this issue. Suppose we have a network G where only information on a subgraph $\tilde{G} = (\mathcal{V}_{\tilde{G}}, \mathcal{E}_{\tilde{G}})$, $\mathcal{V}_{\tilde{G}} \subseteq \mathcal{V}_G$, $\mathcal{E}_{\tilde{G}} \subseteq \mathcal{E}_G$ is available. If the network interventions are constrained to those targeting parts of this subgraph, then also the costs could be computed as above only for the subgraph instead of the complete graph. This approach might be too rough in case of costs based on network functionality though. Another approach would be to estimate the costs by means of the available information on $\tilde{G}$. Suppose to this end that $\tilde{G}$ is representative of G to a certain extend, e.g. because the organisation of G follows some known geometric rules, or that G approximately admits a self-similar structure and $\tilde{G}$ contains information on the connectivity pattern of network clusters in G. Indeed, self-similar properties of networks have been studied and found in the existing literature, see f.e. [62]. Then the desired properties such as graph efficiency or average communicability can possibly be reconstructed from those of $\tilde{G}$:

1. By estimating statistical network properties such as the distributions of node degrees in the network G from the information about $\tilde{G}$, the functionality of G could be approximated using data on similarly structured networks of the same size or by application of some known scaling rules.

2. The missing pieces of network information could otherwise be artificially generated using random graph models with suitable properties. Then the functionality could be determined in an appropriate set of samples.

3. Alternatively, more sophisticated estimation techniques such as network embeddings in hyperbolic surfaces have been applied to networks with substantially incomplete information, see [51] for a recent example. Good results were obtained for the estimation of shortest path lengths between nodes in a range of relevant technology networks, including the internet.

6. Measures of Resilience to Cyber Contagion

Definition 6.1. *A* ***measure of system resilience*** *is a triplet* $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ *where*

- $\mathcal{A}$ *is a network acceptance set,*
- $\mathcal{I}^{\downarrow}$ *is a set of interventions such that* $\mathcal{A}$ *and* $\mathcal{I}^{\downarrow}$ *satisfy Axiom 1,*
- *and* $\mathcal{C}$ *is a cost function for* $(\mathcal{A}, \mathcal{I}^{\downarrow})$ *as in Definition 5.1.*

If $\mathcal{A}$ *is an acceptance set for pandemic cyber contagion, then* $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ *is called a* ***measure of resilience to cyber contagion****.*

Note that a measure of system resilience does a priori

Q1 not answer the question of minimal costs to achieve acceptability (if possible), Q2 nor does it necessarily allow to compare the risk of two or more networks.

The reason for that is—as is well-known from multivariate risk measure theory in mathematical finance—that a satisfactory answer to Q1 and Q2 might be hard to achieve:

- Answering Q1 requires complete knowledge of all possible ways to transform any network into an acceptable state and the related costs to achieve acceptability. For larger networks, this presents a computability and complexity problem that might be difficult or impossible to solve.
- Dealing with Q2 may require to know the answer to Q1. Eventually it is questionable whether Q2 is really of interest, since in most applications in mind the supervisor is managing a *given* network, and is not free to choose an initial configuration to start with. This given network has to be secured somehow in an admissible and ideally efficient way.

However, below we will briefly discuss ways to use a measure of system resilience $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ to construct univariate and set-valued risk measures, thereby also addressing Q1 and Q2.

Remark 6.2. *$\mathcal{I}^{\downarrow}$ is, of course, essential to construct any successful risk reducing strategy to achieve acceptability. But as already mentioned in the discussion of Axiom 1, it is conceivable that efficient strategies may combine risk-reducing and risk-increasing interventions. A regulator who's solely task is to secure a network will probably only consider $\mathcal{I}^{\downarrow}$-strategies. However, a central planner who is concerned with developing a network under security constraints may also consider risk-increasing interventions which enhance network functionality. In particular, this may be the case if a network is acceptable to start with and would allow for some enhancement without loosing acceptability. In that case a set of risk-increasing interventions $\mathcal{I}^{\uparrow}$ comes into play. That is the reason why we for instance discussed properties of the cost function with respect to such a set $\mathcal{I}^{\uparrow}$. Nevertheless, measures of system resilience do not require $\mathcal{I}^{\uparrow}$, for instance when we are only interested in achieving acceptability in a not necessarily optimal or minimal sense. Therefore, $\mathcal{I}^{\uparrow}$ does not directly appear in Definition 6.1, but potentially only implicitly through, e.g., the cost function. Also note that allowing for $\mathcal{I}^{\downarrow} \cup \mathcal{I}^{\uparrow}$-strategies significantly increases the complexity.*

Remark 6.3. *In reality the supervisor may be limited in her ability to intervene. It is common practice in the regulation of cyber security to only target certain industry sectors, and only the most essential network entities within them, but not small companies or private users. For instance, the European Union's NIS2 Directive [23] on the regulation of digital critical infrastructure systems follows a* size-cap rule *that limits the scope of the directive to entities of medium or large size operating in the targeted sectors.*

Hence, the risk management is typically constrained to a set of admissible *interventions. Of course, only such measures of resilience to cyber contagion are reasonable where there are admissible non-trivial interventions in $\mathcal{I}^{\downarrow}$. In order to implement restrictions like the mentioned size-cap rule admissible interventions may be conditional. Conditional means that, for instance, an elementary intervention $\kappa^v_{\cdot}$ on a node v from Section 3.1.1 now takes the form*

$$\tilde{\kappa}^v_{\cdot}(G) := \begin{cases} \kappa^v_{\cdot}(G) & \text{if } v \in Z(G) \\ G & \text{else} \end{cases}$$

where $Z(G) \subset \mathcal{V}_G$ depends on parameters such as a node's size, often measured in terms of its centrality, see Section 6.3. Whether an intervention is admissible may also depend on a particular graph G which the supervisor has to secure. In that case the measure of resilience to cyber contagion may be tailored to handle G, for instance by a specific choice of intervention set $\mathcal{I}^{\downarrow}$, and might not make sense for other graphs, recall Q2 above. For the sake of convenience we keep our discussion of interventions simple, not further mentioning these kind of restrictions in our examples.

6.1. Univariate Risk Measures

Consider a measure of system resilience $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$. A natural way to obtain a univariate risk measure of the form $\rho : \mathcal{G} \to \mathbb{R} \cup \{\infty\}$ is to let $\rho(G)$ denote the infimal cost of achieving acceptability (if possible) for a network G:

$$\rho(G) := \inf\{\mathcal{C}(G, \tilde{G}) | \tilde{G} \in \sigma^{\mathcal{I}^{\downarrow}}(G) \cap \mathcal{A}\}, \quad \text{where } \inf \emptyset := \infty. \tag{12}$$

In case there is also a set of risk-increasing interventions $\mathcal{I}^{\uparrow}$ with respect to which $\mathcal{C}$ satisfies *C5* one could also consider

$$\tilde{\rho}(G) := \inf\{\mathcal{C}(G, \tilde{G}) | \tilde{G} \in (\sigma^{\mathcal{I}^{\downarrow}}(G) \cup \sigma^{\mathcal{I}^{\uparrow}}(G)) \cap \mathcal{A}\}, \quad \text{where } \inf \emptyset := \infty. \tag{13}$$

(13) allows to potentially increase the risk, for instance to enhance functionality, provided the network G is and remains acceptable. (Replacing $\sigma^{\mathcal{I}^{\downarrow}}(G) \cup \sigma^{\mathcal{I}^{\uparrow}}(G)$ by $\sigma^{\mathcal{I}^{\downarrow} \cup \mathcal{I}^{\uparrow}}(G)$ is also conceivable, recall Remark 6.2, but would require further properties of $\mathcal{C}$ to make statements such as in Lemma 6.4 below.)

This approach is in line with the construction of monetary risk measures in financial risk management as in [4], see also [36] for a comprehensive discussion of monetary risk measures. These measures have also been applied to the measurement of systemic financial risks, see for example [11].

Lemma 6.4. *The univariate measure ρ given in* (12) *satisfies*

1. $\rho(G) \geq 0$ *and* $\tilde{\rho}(G) \geq 0$ *for* $G \notin \mathcal{A}$,
2. $\rho(G) = 0$ *and* $\tilde{\rho}(G) \leq 0$ *whenever* $G \in \mathcal{A}$.
3. *Suppose, moreover, that*

$$\inf\{\mathcal{C}(G, \tilde{G}) \mid G \in \mathcal{G}, \tilde{G} \in \sigma^{\mathcal{I}^{\downarrow}}(G) \setminus \{G\}\} > 0. \tag{14}$$

Then $\rho(G) > 0$ *and* $\tilde{\rho}(G) > 0$ *for all* $G \notin \mathcal{A}$ *and in particular* $\mathcal{A} = \{G \in \mathcal{G} \mid \rho(G) = 0\} = \{G \in \mathcal{G} \mid \tilde{\rho}(G) \leq 0\}$.

Proof. 1. immediately follows from property *C2* of the cost function, and from the fact that $\sigma^{\mathcal{I}^{\uparrow}}(G) \cap \mathcal{A} = \emptyset$ whenever $G \notin \mathcal{A}$. As for 2., this follows from $\mathrm{id} \in \mathcal{I}^{\downarrow}$ and thus $G \in \sigma^{\mathcal{I}^{\downarrow}}(G)$, and from $\mathcal{C}(G, G) = 0$ by property *C1*. 3. is easily verified. $\square$

Note that (14) is, for instance, satisfied in the situation of Section 5.1 provided that $\inf\{\tilde{p}(\kappa) \mid \kappa \in \mathcal{I}^{\downarrow} \setminus \{\mathrm{id}\}\} > 0$.

However, as mentioned, while such a construction (12) is possible in theory, it may be difficult or impossible to solve the optimization problem (12) in practice due to the high dimensionality of larger network systems. Furthermore, it is not clear a priori whether the infimum in (12) is a minimum whenever $\rho(G) < \infty$, that is whether there is a "best" acceptable version of the network G.

6.2. Set-Valued Risk Measures

Set-valued measures have been considered in the assessment of systemic risk in financial networks, see, e.g., [33]. A set-valued risk measure comprising the information provided by $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is

$$\rho : \mathcal{G} \to \mathcal{P}(\mathbb{R}), \qquad G \mapsto \{\mathcal{C}(G, \tilde{G}) | \tilde{G} \in \sigma^{\mathcal{I}^{\downarrow}}(G) \cap \mathcal{A}, \mathcal{C}(G, \tilde{G}) \in \mathbb{R}\}. \tag{15}$$

Note that $\rho(G) = \emptyset$ is possible. In a next step one typically searches for efficient strategies to achieve acceptability in terms of lowest possible costs. In the context of financial risk measures, a grid-search approach has been applied for this purpose in [33].

If costs are measured in monetary terms and if these are eventually to be allocated amongst the agents (nodes) of the network, then one could further modify (15) by considering a set of allocations of costs that are necessary for network transformations towards acceptability:

$$\rho : \mathcal{G} \to \bigcup_{d=2}^{\infty} \mathcal{P}(\mathbb{R}^d),$$

$$G \mapsto \left\{ (\mathcal{C}_1, \cdots, \mathcal{C}_d) \in \mathbb{R}^d || \mathcal{V}_G| = d, \exists \tilde{G} \in \sigma^{\mathcal{I}^{\downarrow}}(G) \cap \mathcal{A} : \sum_{i=1}^{d} \mathcal{C}_i = \mathcal{C}(G, \tilde{G}) \in \mathbb{R} \right\}$$

This would be closer to the initial construction of systemic risk measures in [33] where risk is measured in terms of capital requirements of the single financial firms.

6.3. Working with the Triplet $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$

As previously mentioned, in many situations the supervisor is faced with the task of securing a particular existing network G in an admissible manner, see Remark 6.3. Ideally, this should be done as efficiently as possible in terms of low costs, without necessarily having to be (cost) optimal in a strict sense. In this section we discuss some approaches to construct efficient $\mathcal{I}^{\downarrow}$-strategies for G based on the available information about G. We will not consider any optimality properties of those strategies, and in particular not involve risk-increasing strategies. Considerations of this type are left for future research.

A natural approach is to target the *most central nodes* of the network G, because a significant factor triggering the spread of contagious cyber risks is the often observed heterogeneity of the network topology, and in particular the existence of hubs. The findings in [5] suggest that only a small number of highly centralized nodes need to be targeted for an effective protection of the full network, and therefore, the negative impact on the system functionality is quite limited. Note that this strategy in fact corresponds to a common regulatory approach such as the aforementioned size-cap-rule of the NIS2 Directive [23], see Remark 6.3, and should therefore be admissible in practical applications.

In order to target the most central nodes, we need to clarify what we actually mean by the term *central*. In the literature a large variety of different centrality measures has been proposed, see Chapter 7.1 in [56] for a comprehensive overview. We briefly discuss some selected version of centrality in the following:

6.3.1. Node Centralities

A *node centrality measure* is a map

$$\mathfrak{C}^n : \mathbb{V} \times \mathcal{G} \to \mathbb{R}_+ \cup \{\emptyset\} \qquad \text{such that} \quad \mathfrak{C}(v, G) = \emptyset \Leftrightarrow v \notin G.$$

The most prominent examples fall in either one of the following two categories:

Degree-Based Centrality Measures The simplest way to measure the centrality of a node is by its in-, out- or total degree:

$$\mathfrak{C}^{deg}_{in}(v, G) = k_v^{G,in}, \quad \mathfrak{C}^{deg}_{out}(v, G) = k_v^{G,out}, \quad \mathfrak{C}^{deg}(v, G) = k_v^G.$$

Determining degree centralities in a network only requires *local information* on the single nodes. Thus, one advantage of this simple construction is that the centrality for the important parts of the network can also be assessed under incomplete information as long as the nodes with the highest degrees are known, which seems reasonable. Moreover, the simulation studies carried out in [5] indicate that this simple procedure already performs reasonably well.

There are a number of extensions of the concept of degree centrality where connections to high-degree nodes are more important than those to nodes with a low degree level. Usually, this leads to a definition of centrality that is based on the entries of the normalized (left or right) eigenvector associated with the largest eigenvalue of the adjacency matrix, see Section 7.1 in [56] for details. However, determining this kind of centralities poses a problem in presence of incomplete information as they are calculated from the full adjacency matrix of the graph.

Path-Based Centrality Measures This latter issue also arises when other types of node centrality measures, where centrality is not defined by node degrees but via shortest paths, are applied. A simple construction is given by *in-* or *out-closeness centrality*, which calculates the average distance from a node to others, either in terms of incoming or outgoing paths:

$$\mathfrak{C}_{in}^{close}(v,G) = \frac{1}{|\mathcal{V}_G|-1}\sum_{w\neq v}\frac{1}{l_{wv}^G}, \quad \mathfrak{C}_{out}^{close}(v,G) = \frac{1}{|\mathcal{V}_G|-1}\sum_{w\neq v}\frac{1}{l_{vw}^G} \tag{16}$$

in case $|\mathcal{V}_G| \geq 2$ and $\mathfrak{C}_{in}^{close}(v,G) = \mathfrak{C}_{out}^{close}(v,G) = 0$ whenever $G = (\{v\},\emptyset)$.

The most prominent example of a path-based centrality measure in the literature is given by the *betweenness centrality*

$$\mathfrak{C}^{\mathrm{bet}}(v,G) = \sum_{\substack{u,w\\ u,w\neq v}}\frac{\sigma_{uw}(v)}{\sigma_{uw}}, \tag{17}$$

where σ_{uw} denotes the total number of shortest paths from node u to w, and $\sigma_{uw}(v)$ is the number of these paths that go through node v, and where we set $0/0 := 0$.[11] Although in [5] strategies based on betweenness centrality slightly outperformed those based on degree centrality, the aforementioned information problem may pose a significant drawback in practical applications. Moreover, the sets of the most central nodes under betweenness or degree centrality are likely to coincide to a large extent, so that the resulting intervention strategies would look fairly similar.

6.3.2. Edge Centralities

Instead of focussing on the nodes, we can also consider *edge centrality measures*

$$\mathfrak{C}^e : \mathbb{E}\times\mathcal{G} \to \mathbb{R}_+ \cup \{\emptyset\} \qquad \text{where} \quad \mathfrak{C}((v,w),G) = \emptyset \Leftrightarrow (v,w) \notin \mathcal{E}_G.$$

The most prominent example is the *edge betweenness centrality*, first proposed in [41], where, in analogy to the corresponding node centrality measure, centrality of an edge (q,r) is measured by the number of shortest paths $\sigma_{vw}((q,r))$ between any two nodes v and w that pass through (q,r), in relation to the total number of paths σ_{vw} between these two nodes:

$$\mathfrak{C}^{edge}((q,r),G) = \sum_{v,w\in\mathcal{V}_G}\frac{\sigma_{vw}((q,r))}{\sigma_{vw}}$$

where we set $0/0 := 0$. As in the case of node betweenness centrality, edge betweenness centrality requires full information about the network topology, which might not be accessible. Also note that centrality measures for edges are not as widely represented in the literature as node centralities.

[11] Note that slightly different definitions can be found in the literature, f.e., in [56], where also paths with $u = v$ or $w = v$ are considered. However, we follow the definition from [9] here which is commonly used in algorithmic implementations like the NetworkX package for Python or in MATLAB.

6.3.3. Targeted Strategies for a Given Network

A reasonable procedure now is as follows: Pick a node centrality measure $\mathfrak{C}^n$ and assume that at least the most central nodes of the given network G according to $\mathfrak{C}^n$ are known.

1. Rank the nodes of G according to $\mathfrak{C}^n$.
2. Pick the most central node v and choose some network intervention from $\kappa \in \mathcal{I}^{\downarrow}$ changing the node v or its incoming and outgoing edges. The choice of κ may depend on the cost $\mathcal{C}(G, \kappa(G))$.
3. If κ also requires a choice of edges which are affected, as in the case of node splitting, pick the edges according to an edge centrality measure $\mathfrak{C}^e$ if possible, or use some other information if available, or simply choose randomly.
4. Check whether $\kappa(G) \in \mathcal{A}$. If this is the case, then stop, otherwise go back to step 1 (or discard the strategy if we have not stopped after a specified number of iterations).
5. If in the previous step we stop, compute the cost of transforming the initial network into the now acceptable configuration.
6. Repeat the previous procedure 1.–5. for different choices of $\kappa \in \mathcal{I}^{\downarrow}$ in step 2. Compare the costs of the resulting $\mathcal{I}^{\downarrow}$-strategies for achieving acceptability, and choose the cheapest strategy.

An implementation of the described procedure to achieve acceptability based on artificial learning algorithms is part of future research.

7. Examples

The examples presented in this section will all be based on network acceptance sets $\mathcal{A}$ of the form

$$\mathcal{A} = \{G \in \mathcal{G} | Q(G) \leq l_{|\mathcal{V}_G|}\}, \tag{18}$$

where a specific network quantity $Q : \mathcal{G} \to \mathbb{R} \cup \{-\infty, \infty\}$ needs to be bounded for acceptability of a network G, and the bounds $l_N \in \mathbb{R}$, $N \in \mathbb{N}$, depend on the network size N.

Definition 7.1. *Let $\mathcal{I}$ be a non-empty set of network interventions and let $Q : \mathcal{G} \to \mathbb{R} \cup \{-\infty, \infty\}$. We call Q $\mathcal{I}$-monotone if $Q(\kappa(G)) \leq Q(G)$ for all $G \in \mathcal{G}$ and $\kappa \in \mathcal{I}$.*

The following lemma is easily verified.

Lemma 7.2. *Suppose that Q is $\mathcal{I}$-monotone. Then*

1. *$Q(\kappa(G)) \leq Q(G)$ for all $G \in \mathcal{G}$ and $\kappa \in [\mathcal{I}]$,*
2. *$\mathcal{I}$ is risk-reducing for $\mathcal{A}$.*

If, moreover, $\mathcal{I}$ is not partially self-revers, then $\mathcal{I}$-monotonicity is the same as Q being decreasing with respect to the partial order $\preccurlyeq_{\mathcal{I}}$ given in Proposition 3.9.

In case $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$ one should expect that Q is indeed $\mathcal{I}^{\downarrow}$-monotone. In the following examples the function Q depends on moments of the degree distribution. This is motivated by the well-known fact that those moments have a significant influence on the epidemic vulnerability of networks, see the discussion in Section 1.

7.1. Controlling Moments of Degree Distributions

Given a network $G \in \mathcal{G}$, we let $P_G^{out}(k)$ denote the fraction of nodes v with out-degree k, or, equivalently, the probability that a node v which is chosen uniformly at random comes with $k_v^{G,out} = k$. The corresponding distribution P_G^{out} over all possible degrees is called the *out-degree distribution* of the network G. Analogously, we can define the *in-degree distribution* P_G^{in}. Let K_G^{out} denote a random variable which represents the out-degree of a randomly chosen node given the probability distribution P_G^{out}, i.e. $\mathbb{P}(K_G^{out} = k) = P_G^{out}(k)$ for all $k = 0, 1, \dots, |\mathcal{V}_G| - 1$. We define K_G^{in} analogously. The *n-th moment* of the in- and out-degree distributions are given by

$$\mathbb{E}\big[(K_G^{in})^n\big] := \sum_{k\in\mathbb{N}_0} k^n P_G^{in}(k), \quad \mathbb{E}\big[(K_G^{out})^n\big] := \sum_{k\in\mathbb{N}_0} k^n P_G^{out}(k), \quad n \in \mathbb{N}.$$

Clearly any network acceptance set such that Q only depends on the degree-distribution is topological invariant:

Lemma 7.3. *If $\mathcal{A}$ is given by* (18) *where Q only depends on the in-, out-degree distribution, then $\mathcal{A}$ satisfies Axiom 6. Moreover, if $Q(G) = \mathbb{E}\big[(K_G^{out})^n\big]$, or $Q(G) = \mathbb{E}\big[(K_G^{in})^n\big]$, $G \in \mathcal{G}$, for some $n \in \mathbb{N}$ and the sequence of bounds $(l_N)_{N\in\mathbb{N}}$ is non-decreasing in N, then $\mathcal{A}$ satisfies Axiom 5.*

Proof. The first statement is trivial. Moreover, regarding Axiom 5 consider two networks G of size N and H of size M with disjoint vertex sets and a non-decreasing sequence $(l_N)_{N\in\mathbb{N}}$. Then the disjoint graph union $G \cup H$ satisfies

$$\mathbb{E}[(K_{G\cup H}^{in})^n] = \frac{1}{N+M}(N\mathbb{E}[(K_G^{in})^n] + M\mathbb{E}[(K_H^{in})^n]) \leq \frac{1}{N+M}(N \cdot l_N + M \cdot l_M) \leq l_{N+M},$$

and similarly for the out-degree. $\square$

Remark 7.4. *As will be verified by the following examples, for the management of cyber pandemic risk, the distribution of outgoing, not incoming, node degrees is the relevant entity. This is in line with our formulation of Axiom 4 and motivated by the fact that an infection of a node with high out-degree can easily spread to a substantial fraction of the network, which in contrast is not the case for nodes which solely come with a high number of incoming edges.*

7.1.1. Variance of Degree Distributions

In the following we show that the variance of either in- or out-degree distributions is not a satisfactory control.

Proposition 7.5. *Suppose that the network acceptance set $\mathcal{A}$ satisfies* (18) *where Q equals the variance of either the in- or out-degree distribution, and that $l_N \geq 0$ for all $N \in \mathbb{N}$. In both cases, $\mathcal{A}$ satisfies Axioms 2, but violates Axiom 4'. If Q equals the variance of the out-degree distribution, then $\mathcal{A}$ violates Axiom 4. Moreover, Q is not $\mathcal{I}$-monotone for any choice of $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{e\_add} \cup \mathcal{I}_{n\_del} \cup \mathcal{I}_{n\_add}$ such that $\mathcal{I} \neq \emptyset$, that is for no non-trivial set of elementary network interventions.*

Proof. The in- and out-degree distributions of all edgeless and all complete graphs have zero variance. Thus, Axiom 2 is always satisfied while Axiom 4' is violated. The out-degree distribution of all graphs such that any node has an out-going edge to any other node has zero variance. Hence, if Q equals the variance of the out-degree distribution, then Axiom 4 is violated.

As regard the monotonicity of Q, variance, of either the in- our out-degree distribution, increases by adding edges to the edgeless graph, or by deleting edges in the complete graph. Moreover, the variance of a complete graph increases when adding an isolated node to the network. As regards, note that also any network $G^\circ = (\mathcal{V}_{G^\circ}, \mathcal{E}_{G^\circ})$ with a bidirectional ring topology, that is a circular graph with $\mathcal{V}_{G^\circ} = \{v_1, \cdots, v_N\}$ and

$$\mathcal{E}_{G^\circ} = \{(v_1, v_2), (v_2, v_1), \cdots, (v_{N-1}, v_N), (v_N, v_{N-1}), (v_N, v_1), (v_1, v_N)\},$$

see Figure 6, comes with a zero variance for both in- and out-degree distributions since each node has the in- and out-degree 2. However, when deleting node v_N, the network equals the line network, see Figure 6, with vertex set $\{v_1, \cdots, v_{N-1}\}$ and edges

$$\{(v_1, v_2), (v_2, v_1), \cdots, (v_{N-2}, v_{N-1}), (v_{N-1}, v_{N-2})\}.$$

If $N \geq 4$, in contrast to all the other nodes, v_1 and v_{N-1} only have one incoming and one outgoing edge. Therefore, the variance of both the in- and out-degree distribution now is positive. $\square$

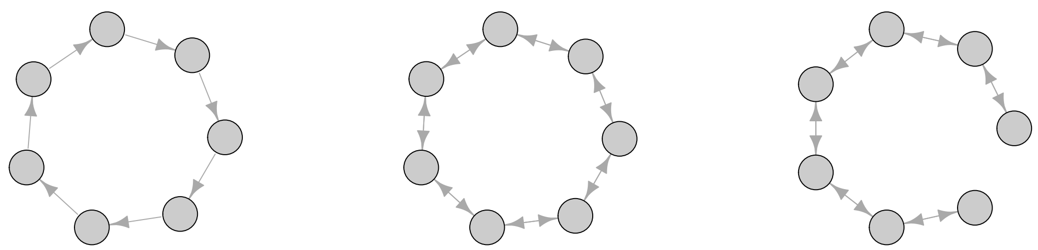

Figure 6: A directed (left) and a bidirectional (middle) ring graph, and a bidirectional line network (right), all consisting of $N = 7$ nodes.

7.1.2. Average Degrees

Next we consider the *average in-* and *-out degree* of a network G. Note that these first moments are equal since every edge that emanates from a node v needs to arrive at another one, that is we have

$$\mathbb{E}[K_G^{in}] = \frac{1}{N}\sum_{i=1}^{N} k_{v_i}^{G,in} = \frac{|\mathcal{E}_G|}{|\mathcal{V}_G|} = \frac{1}{N}\sum_{i=1}^{N} k_{v_i}^{G,out} = \mathbb{E}[K_G^{out}]. \tag{19}$$

Proposition 7.6. *Consider $\mathcal{A}$ as in* (18) *with $Q(G) = \mathbb{E}[K_G^{out}](= \mathbb{E}[K_G^{in}])$. Then Q is $\mathcal{I}$-monotone for any $\mathcal{I}$ that is composed of edge deletions and node splittings, i.e. $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split}$. Hence, $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^\downarrow$ whenever $\{\mathrm{id}\} \subsetneq \mathcal{I}^\downarrow \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\mathrm{id}\}$.*

Proof. The result follows directly from Equation (19): For any $\kappa \in \mathcal{I}_{e\_del}$ and network G we have that $|\mathcal{V}_{\kappa(G)}| = |\mathcal{V}_G|$ and $|\mathcal{E}_{\kappa(G)}| \leq |\mathcal{E}_G|$. In case of node splittings $\kappa \in \mathcal{I}_{n\_split}$ we have $|\mathcal{E}_{\kappa(G)}| = |\mathcal{E}_G|$ and $|\mathcal{V}_{\kappa(G)}| \geq |\mathcal{V}_G|$. $\square$

Corollary 7.7. *Suppose that $\mathcal{I}^\downarrow$ satisfies $\{\mathrm{id}\} \subsetneq \mathcal{I}^\downarrow \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\mathrm{id}\}$, and suppose that $l_{N_0} \geq 0$ for some $N_0 \in \mathbb{N}$. Then, $\mathcal{A}$ is a topology invariant network acceptance set which also satisfies Axiom 5 whenever $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing. $(\mathcal{A}, \mathcal{I}^\downarrow, \mathcal{C})$ is a measure of system resilience for any cost function $\mathcal{C}$ for $(\mathcal{A}, \mathcal{I}^\downarrow)$.*

Proof. Combine Proposition 7.6 with Lemma 7.3. Note that $l_{N_0} \geq 0$ for some $N_0 \in \mathbb{N}$ ensures that $\mathcal{A}$ is non-empty. $\square$

Lemmas 5.8 and 5.10 show that apart from monetary costs, the cost function $\mathcal{C}$ in Proposition 7.6 can be based on a loss of network functionality such as in Section 5.2. Communicability-based costs work for any choice of $\mathcal{I}^{\downarrow}$ as in Proposition 7.6 , whereas costs based on shortest paths require a further restriction of $\mathcal{I}^{\downarrow}$ to be a subset of $\mathcal{I}_{e\_del}$.

The average node degree only provides a measure of overall graph connectivity in the mean, considering the number of edges in comparison to the number of nodes. However, it does not evaluate characteristics which relate closer to the topological arrangement of edges within the network, that is for example the presence hubs which may act as risk amplifiers. Networks can have a very different risk profile, even if they contain the same number of edges and nodes, see for example the analysis in [5]. Hence, one may doubt whether acceptance sets given by $Q(G) = \mathbb{E}[K_G^{out}] (= \mathbb{E}[K_G^{in}])$ are reasonable choices. And indeed, the following Proposition 7.8 shows that if $Q(G) = \mathbb{E}[K_G^{out}]$, $\mathcal{A}$ cannot satisfy Axioms 3 and 4 simultaneously.

Proposition 7.8. *An acceptance set as in* (18) *with* $Q(G) = \mathbb{E}[K_G^{out}] (= \mathbb{E}[K_G^{in}])$ *cannot satisfy the Axioms 3 and 4 simultaneously. More precisely, if Axiom 3 is satisfied, then Axiom 4 is violated, and vice versa.*

Proof. Consider a strongly connected network G of size N. Then for every node pair $v, w \in \mathcal{V}_G$ we find a path from v to w and vice versa. Hence, in particular $k_v^{G,out}, k_v^{G,in} \geq 1$ for all $v \in \mathcal{V}_G$. As $\sum_{i=1}^N k_{v_i}^{G,in} = \sum_{i=1}^N k_{v_i}^{G,out} = |\mathcal{E}_G|$, this implies that G contains at least N edges so that $Q(G) \geq 1$, recall (19). However, a directed star graph G^* of size N only contains $|\mathcal{V}_{G^*} \setminus \{v^*\}| = N-1$ edges, and therefore, its first moment is $Q(G^*) = (N-1)/N < 1$. Therefore, if a strongly connected network is acceptable, then the directed star graph of the same size is also acceptable. The latter constitutes a violation of Axiom 4. Conversely, if Axiom 4 is satisfied, so in particular no directed star graph is acceptable, then we cannot have any acceptable strongly connected graph. $\square$

Hence, the average degree is not suited for constructing a measure of resilience to cyber contagion.

Remark 7.9. *Proposition 7.8 also implies that a simple control such as limiting the total number of edges* $Q(G) = |\mathcal{E}_G|$ *by a fixed constraint* $l \in \mathbb{N}$*, irrespective of the network size* N*, does not define an acceptance set for cyber pandemics: indeed, this is simply a special case of controlling the first moment of degree distributions with constraints* $l_N = l/N$*, see* (19).

7.1.3. Second Moments

Proposition 7.10. *Consider* $\mathcal{A}$ *as in* (18) *with* $Q(G) = \mathbb{E}[(K_G^{out})^2]$ *or* $Q(G) = \mathbb{E}[(K_G^{in})^2]$*. Then* Q *is* $\mathcal{I}^{\downarrow}$*-monotone for any* $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\mathrm{id}\}$*. Hence* $\mathcal{A}$ *satisfies Axiom 1 with any such* $\mathcal{I}^{\downarrow}$ *such that* $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$*.*

Proof. Clearly, the second moments are reduced when deleting edges in a network. Further, the second moment of the in- or out-degree distribution is also decreasing under node splitting: Let v be the node in a network G of size N which is split into v and $\tilde{v}$, and $\tilde{G}$ the resulting network. Due to $k_v^{G,in} = k_v^{\tilde{G},in} + k_{\tilde{v}}^{\tilde{G},in}$ and $k_v^{G,out} = k_v^{\tilde{G},out} + k_{\tilde{v}}^{\tilde{G},out}$, we have

$$(k_v^{\tilde{G},in})^2 + (k_{\tilde{v}}^{\tilde{G},in})^2 \leq (k_v^{\tilde{G},in})^2 + (k_{\tilde{v}}^{\tilde{G},in})^2 + 2k_v^{\tilde{G},in} k_{\tilde{v}}^{\tilde{G},in} = (k_v^{\tilde{G},in} + k_{\tilde{v}}^{\tilde{G},in})^2 = (k_v^{G,in})^2, \tag{20}$$

and thus

$$\begin{aligned}\mathbb{E}[(K_{\tilde{G}}^{in})^2] &= \frac{1}{N+1}\Big(\sum_{w \neq v, \tilde{v}} (k_w^{\tilde{G},in})^2 + (k_v^{\tilde{G},in})^2 + (k_{\tilde{v}}^{\tilde{G},in})^2\Big) \\ &\leq \frac{1}{N}\left(\sum_{w \neq v, \tilde{v}} (k_w^{\tilde{G},in})^2 + (k_v^{G,in})^2\right) = \frac{1}{N}\left(\sum_{w \neq v, \tilde{v}} (k_w^{G,in})^2 + (k_v^{G,in})^2\right) = \mathbb{E}[(K_G^{in})^2].\end{aligned}$$

$\square$

Proposition 7.11. *Consider a network acceptance set* $\mathcal{A}$ *as in* (18) *with* $Q(G) = \mathbb{E}\big[(K_G^{out})^2\big]$ *or* $Q(G) = \mathbb{E}\big[(K_G^{in})^2\big]$.

1. $\mathcal{A}$ *satisfies Axiom 2 if and only if* $l_N \geq 0$ *for all* $N \geq 2$,
2. $\mathcal{A}$ *satisfies Axiom 3 if and only if there is a* $N_0 \in \mathbb{N}$ *such that* $l_N \geq 1$ *for all* $N \geq N_0$,
3. *If* $Q(G) = \mathbb{E}\big[(K_G^{out})^2\big]$, *then* $\mathcal{A}$ *satisfies Axiom 4 if and only if* $l_N < (N-1)^2/N$ *for all* $N \geq 1$.
4. *If* $Q(G) = \mathbb{E}\big[(K_G^{in})^2\big]$, *then* $\mathcal{A}$ *cannot satisfy the Axioms 3 and 4 simultaneously. More precisely, Axiom 3 implies that Axiom 4 is violated and vice versa.*

Proof. 1. The second moment of the (out- or ingoing) node degrees of any edgeless graph equals zero by definition.

2. We only prove the assertion for the out-degree distribution, The same proof holds true in case of the in-degree distribution. Since $k \leq k^2$ for all $k \in \mathbb{N}$, we find that

$$\mathbb{E}\big[(K_G^{out})^2\big] \geq \frac{1}{N} \sum_{v \in \mathcal{V}_G} k_v^{G,out} = \frac{|\mathcal{E}_G|}{N} = \mathbb{E}\big[K_G^{out}\big]$$

for any network G of size N. Recall that a strongly connected network G of size N contains at least N edges, see the proof of Proposition 7.8. Therefore, any strongly connected network G satisfies

$$\mathbb{E}\big[(K_G^{out})^2\big] \geq 1. \tag{21}$$

Equality in (21) is realized by every directed ring network G° with $\mathcal{V}_{G^\circ} = \{v_1, \cdots, v_N\}$ and $\mathcal{E}_{G^\circ} = \{(v_1, v_2), \cdots, (v_{N-1}, v_N), (v_N, v_1)\}$, where each node is associated with exactly one outgoing edge as in Figure 6. Indeed, $\mathbb{E}\big[(K_{G^\circ}^{out})^2\big] = 1$, irrespective of the network size N. Therefore, $\mathcal{A}$ contains a strongly connected graph if and only if $\mathcal{A}$ contains a (and thus every) directed ring network of the same size, and the latter is equivalent to the existence of $N_0 \in \mathbb{N}$ such that $l_N \geq 1$ for all $N \geq N_0$.

3. According to Proposition 7.10, Q is $\mathcal{I}_{e\_del}$-monotone. Therefore, it suffices to consider the networks which contain a super-spreader but otherwise have minimal amount of edges, that is the directed star graphs. The second moment of the out-degree distribution of a directed star graph G^* of size N is given by

$$\mathbb{E}\big[(K_{G^*}^{out})^2\big] = \frac{1}{N}\big(1 \cdot (N-1)^2 + (N-1) \cdot 0\big) = \frac{(N-1)^2}{N}.$$

4. As above we obtain that

$$\mathbb{E}[(K_G^{in})^2] \geq \frac{|\mathcal{E}_G|}{N}$$

for any network G of size N. Consider any strongly connected network G with N nodes for some $N \in \mathbb{N}$. Then G contains at least N edges (again see proof of Proposition 7.8). Hence, $\mathbb{E}[(K_G^{in})^2] \geq 1$. A directed star graph G^* of size N only contains $N-1$ edges and thus satisfies

$$\mathbb{E}[(K_{G^*}^{in})^2] = \frac{1}{N}((N-1) \cdot 1 + 1 \cdot 0) < 1,$$

because the super-spreader has in-degree 0, and all the other nodes come with a in-degree of 1. Hence, acceptability of a strongly connected graph of size N implies $l_N \geq 1$ and thus that the directed star graph of the same size is acceptable, which violates Axiom 4. Conversely, if we exclude any directed star graph, then necessarily $l_N < 1$ for all $N \in \mathbb{N}$, so there cannot be an acceptable strongly connected graph. Hence, Axiom 3 is violated.

□

Corollary 7.12. *Suppose that the sequence $(l_N)_{N\in\mathbb{N}}$ satisfies $l_1 < 0$, $0 \leq l_N < \frac{(N-1)^2}{N}$ for all $N \geq 2$, and there is $N_0 \geq 3$ such that $l_N \geq 1$ whenever $N \geq N_0$. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\mathrm{id}\}$ such that $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G} | \mathbb{E}[(K_G^{out})^2] \leq l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 5. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

Proof. Combine Propositions 7.10 and 7.11 with Lemma 7.3. □

As in the case of average degrees, Lemmas 5.8 and 5.10 show that, apart from monetary costs, the cost function $\mathcal{C}$ in Corollary 7.12 can be based on a loss of network functionality as in Section 5.2. Communicability-based costs work for any choice of $\mathcal{I}^{\downarrow}$, whereas costs measured by means of shortest paths require that $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del}$. While the second moment of the in-degree distribution is not suited for the construction of measures of resilience to cyber contagion, similar to the case of average degrees, it yields a measure of system resilience by Proposition 7.10.

Next we consider the total degree distribution $K_G := \frac{1}{2}(K_G^{in} + K_G^{out})$.

Proposition 7.13. *Consider a network acceptance set $\mathcal{A} \subset \mathcal{G}$ as in* (18) *with $Q(G) = \mathbb{E}[(K_G)^2]$. Then*

1. *Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\mathrm{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$.*
2. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$,*
3. *$\mathcal{A}$ satisfies Axiom 3 if and only if there is a N_0 such that $l_N \geq 1$ for all $N \geq N_0$.*
4. *$\mathcal{A}$ satisfies Axiom 4 if and only if $l_N < (1/4)(N-1)$ for all $N \geq 1$,*
5. *$\mathcal{A}$ satisfies Axiom 4' if and only if $l_N < N - 1$ for all $N \geq 1$, and in case that there is a $N \in \mathbb{N}$ with $l_N \geq (1/4)(N-1)$, then we must have a $N_0 < N$ with $l_{N_0} \geq 1$.*

Proof. 1.–3. are straightforward modifications of the proof of the corresponding results in Propositions 7.10 and 7.11.
4. and 5.: The second moment of total degrees in a directed star graph G^* of size N equals

$$\mathbb{E}[(K_{G^*})^2] = \frac{1}{N}\Big(1 \cdot (\frac{1}{2}(N-1))^2 + (N-1) \cdot (\frac{1}{2})^2\Big) = \frac{1}{4N}((N-1)^2 + (N-1)) = \frac{N-1}{4}.$$

For the bidirectional star graph of size N we obtain

$$\mathbb{E}[(K_{G^*})^2] = \frac{1}{N}\Big(1 \cdot (N-1)^2 + (N-1) \cdot 1^2\Big) = \frac{1}{N}((N-1)^2 + (N-1)) = N - 1.$$

□

Similar to Corollary 7.12 we obtain:

Corollary 7.14. *Suppose that the sequence $(l_N)_{N\in\mathbb{N}}$ satisfies the constraints given by 2.–4. or by 2.,3., and 5. of Proposition 7.13. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\mathrm{id}\}$ such that $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G} | \mathbb{E}[(K_G)^2] \leq l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 5. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

Recall the epidemic threshold from (1) which would suggest not only to control the second moment of the degree distribution, but indeed a ratio of the second and the first moments. However, note that the epidemic threshold holds for undirected networks. Therefore, we postpone this example to Appendix B.2.3 where we discuss the case of undirected networks in more detail.

7.2. Further Examples

Further examples of measures of resilience to cyber contagion based on a control of the centrality of nodes are collected in Appendix A. Some examples specific to undirected network are provided in Appendix B.

8. Outlook

In the following we collect a number of open questions and challenges for future research:

- *Calibration to Real World Networks:* While this study provides the theoretical foundation and also presents fist stylized examples of measures of resilience to cyber contagion, the next step is to apply such risk measures to managing real world networks. In this context particularly suitable measures of resilience to cyber contagion will be identified together with important parameters such as a desired minimal levels of network functionality, the border between acceptability and non-acceptability in practise (apart from the obvious cases mentioned in the Axioms), etc.

- *Computational Challenges:* Computational problems stem primarily from the high-dimensionality of the networks. Determining suitable or even optimal network manipulations may therefore be challenging. A possible solution may be to develop new machine learning-based algorithms to identify good, not necessarily strictly optimal, ways to secure some given network.

- *Model Uncertainty:* Throughout this paper we frequently addressed the problem that the supervisor might only possess incomplete information about the network she has to secure. Even if we have discussed some basic ideas to overcome this issue, it remains desirable to find a more uniform conceptual handling of model uncertainty in this risk management framework. Such approaches already exist in the area of financial risk measurement, see e.g. [30].

- *Risk Measures based on Infection Models:* An interesting class of risk measures is obtained by choosing an infection model such as the SIR (or SIS) model mentioned in the introduction, see [50], and controlling the scale of an infection in the network determined by the fixed infection model.

- *Weighted Networks:* A weighted network is a network as discussed throughout this paper where in addition weights on the edges describe the degree of transmissibility of some shock through the respective edges. Clearly, a network model may benefit from adding edge weights. However, it might be difficult to determine what actually constitutes these weights and eventually the size of these weights. In order to extend the previously developed framework to weighted graphs, larger modifications are necessary: First of all, network interventions may now also target the edge weights, such as an increase or decrease of a particular edge weight. As regards the axioms for the acceptance set, Axioms 1, 2, 5 and 6 apply also to weighted networks. However, it is less clear how the acceptability of strongly connected graphs in Axiom 3 and non-acceptability of super-spreaders in Axiom 4 are meaningfully generalised to weighted graphs. For instance, the non-acceptability of networks with super-spreaders should also depend on the edge weights associated with the super-spreader node(s). One could specify thresholds for that purpose. However, a rigorous extension of the risk management approach presented in this paper to the case of weighted graphs remains subject of future research.

- *Conditional and Spatial Risk Measures:* It could be reasonable to consider spatial restrictions or conditioning. In particular, restrictions to certain subgraphs of large systems may be of interest for risk managers of individual firms or single network clusters. Conditional risk measures can be considered, for example, in relation to the admissibility of interventions or when making assumptions about the network topology in presence of model uncertainty.

- *Cyber Risk and Financial Stability:* The impact of cyber risk on financial stability can be analyzed using cyber mappings between the cyber and the financial network as illustrated in Figure 1. The risk measures discussed in this paper can be applied to manage the risk in the operational cyber network, or in both networks together, if they can be interpreted as a joint network system. For a profound mathematical analysis, however, it is necessary to create a precise mathematical model description of cyber mappings, and this may require more complex models such as *multi-layer networks*. An extension of the framework presented here to such structures is likely to be significant for macroprudential risk management.

- *Area of Application:* On the most basic level this paper introduces risk measures for complex interconnected systems targeting the underlying network structure. Then we apply this idea to specifically considering risk measures for systemic cyber risk. In the future, it would be interesting to explore applications to a variety of other examples of critical infrastructure networks such as power grids, transportation systems, and production networks.

Appendix A Hub Control via Maximal Centralities

In this section we consider as control Q in (18) the maximal centrality of nodes, thereby limiting the size of hub nodes within the network. To this end, we choose a node centrality measure $\mathfrak{C}$ as discussed in Section 6.3.1, and let

$$Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}(v, G). \tag{22}$$

A.1 In-, Out-, and Total Degree Centrality

Proposition A.1. *Consider an acceptance set $\mathcal{A}$ as in* (18) *with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{out}(v, G)$ or $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{in}(v, G)$. Then Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\text{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\text{id}\} \subsetneq \mathcal{I}^{\downarrow}$.*

Proof. Clearly, deleting an edge does not increase the in- or out-degree of any node in a graph G. The same holds when an arbitrary node split is applied. □

Proposition A.2. *Consider $\mathcal{A} \subset \mathcal{G}$ as in* (18) *with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{out}(v, G)$ or $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{in}(v, G)$. Then*

1. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$,*
2. *$\mathcal{A}$ satisfies Axiom 3 if and only if there is a N_0 such that $l_N \geq 1$ for all $N \geq N_0$.*
3. *If $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{out}(v, G)$, then $\mathcal{A}$ satisfies Axiom 4 and 4' if and only if $l_N < N - 1$ for all $N \geq 1$.*
4. *If $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{in}(v, G)$, then $\mathcal{A}$ cannot satisfy Axioms 3 and 4 simultaneously. More precisely, Axiom 3 implies that Axiom 4 is violated and vice versa.*

Proof.

1. The in- and out-degree of every node in an edgeless graph equals zero.
2. If a network $G \in \mathcal{G}$ with $|\mathcal{V}_G| \geq 2$ is strongly connected, then $|\mathcal{N}_v^{G,out}|, |\mathcal{N}_v^{G,in}| \geq 1$ for all $v \in \mathcal{V}_G$ by definition. Otherwise there would be no path in G via which the node v can be reached, or no other node could be reached from v, respectively. This proves necessity. Sufficiency follow from the bidirectional ring graph of size N (see Figure 6) being an element of $\mathcal{A}$ for any $N \geq N_0$.
3. The out-degree of both a super-spreader and a star node equals $N - 1$ by definition. In particular, this implies that Axiom 4 and 4' are equivalent for the given choice of Q.
4. Q is $\mathcal{I}_{e\_del}$-monotone according to Proposition A.1. For the violation of Axiom 4', it thus suffices to consider the edge-minimal networks with a super-spreader. These are the directed star graphs. For a directed star graph G^* of size $|\mathcal{V}_{G^*}| \geq 2$ with super-spreader v^* we find $\mathfrak{C}^{deg}_{in}(v, G) = 1$ for all $v \in \mathcal{V}_G \setminus \{v^*\}$, and $\mathfrak{C}^{deg}_{in}(v^*, G) = 0$, thus $Q(G^*) = 1$. However, for any strongly connected network G with $|\mathcal{V}_G| \geq 2$ we have $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{in}(v, G) \geq 1$, see 2. Hence, 4. follows.

□

Corollary A.3. *Suppose that the sequence $(l_N)_{N \in \mathbb{N}}$ satisfies $l_1 < 0$, $0 \leq l_N < N - 1$ for all $N \geq 2$, and there is $N_0 \geq 3$ such that $l_N \geq 1$ whenever $N \geq N_0$. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\text{id}\}$ such that $\{\text{id}\} \subsetneq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G} | \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{out}(v, G) \leq l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 5. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

Proof. Combine Propositions A.1 and A.2. Clearly, $\mathcal{A}$ is topologically invariant. As for Axiom 5, note that for any disjoint graph union $G \cup H$ we have

$$Q(G \cup H) = \max\{\max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}_{out}(v, G), \max_{v \in \mathcal{V}_H} \mathfrak{C}^{deg}_{out}(v, H)\} = \max\{Q(G), Q(H)\}.$$

□

Moreover, we can also consider the control of the maximal total degree:

Proposition A.4. *Consider a set $\mathcal{A} \subset \mathcal{G}$ as in* (18) *with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}(v, G)$. Then*

1. *Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\mathrm{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$.*

2. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$,*

3. *$\mathcal{A}$ satisfies Axiom 3 if and only if there is a N_0 such that $l_N \geq 1$ for all $N \geq N_0$.*

4. *$\mathcal{A}$ satisfies Axiom 4 if and only if $l_N < (N-1)/2$ for all $N \geq 1$,*

5. *$\mathcal{A}$ satisfies Axiom 4' if and only if $l_N < N - 1$ for all $N \geq 1$, and in case that there is a $N \in \mathbb{N}$ with $l_N \geq (N-1)/2$, then we must have a $N_0 < N$ with $l_{N_0} \geq 1$.*

Proof. 1.-3. are straightforward modifications of the corresponding results in Propositions A.1 and A.2.
4. and 5.: The total degree of a super-spreader v^* in a directed star graph G^* equals

$$k^{G^*}_{v^*} = \frac{1}{2}(k^{G^*,in}_{v^*} + k^{G^*,out}_{v^*}) = \frac{1}{2}(0 + |\mathcal{V}_G| - 1) = \frac{|\mathcal{V}_G| - 1}{2}.$$

For a star node v^* in a bidirectional star graph G^* we obtain

$$k^{G^*}_{v^*} = \frac{1}{2}(k^{G^*,in}_{v^*} + k^{G^*,out}_{v^*}) = \frac{1}{2}(|\mathcal{V}_G| - 1 + |\mathcal{V}_G| - 1) = |\mathcal{V}_G| - 1.$$

□

Consequently, we obtain the following result in analogy to Corollary A.3:

Corollary A.5. *Suppose that the sequence $(l_N)_{N \in \mathbb{N}}$ satisfies the constraints given by 2.-4. or by 2., 3., and 5. of Proposition A.4. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{n\_split} \cup \{\mathrm{id}\}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G} | \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}(v, G) \leq l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 5. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

A.2 In- and Out-Closeness Centrality

We first note that for path-based centrality meaasures node splits may indeed worsen the situation.

Example A.6. *Consider again the setting from Example 5.9. For all nodes $v = a, b, c$ from the initial network component G_1, we have*

$$\mathfrak{C}_{in}^{close}(v, G) = \mathfrak{C}_{out}^{close}(v, G) = \frac{1}{N-1}\Big(\frac{1}{1} + \frac{1}{1}\Big) = \frac{2}{N-1}.$$

Now, after the node split, the nodes a and c come with in- and out-closeness centralities of

$$\mathfrak{C}_{in}^{close}(v, H) = \mathfrak{C}_{out}^{close}(v, H) = \frac{1}{N}\Big(\frac{1}{1} + \frac{1}{1} + \frac{1}{2}\Big) = \frac{5}{2N}, \quad v = a, c,$$

and we find that

$$\max_{v \in \mathcal{V}_G} \mathfrak{C}_{*}^{close}(v, G) < \max_{v \in \mathcal{V}_H} \mathfrak{C}_{*}^{close}(v, H) \Leftrightarrow \frac{2}{N-1} < \frac{5}{2N} \Leftrightarrow 5 < N, \quad v = a, c,$$

for $* = in, out$. Thus, the maximal in- and out-closeness centrality is increased under the node split if the component G_2 consists of at least three isolated nodes.

Similarly, the betweenness centrality as defined in (17) of all nodes $v \in \mathcal{V}_{G_1}$ equals zero. However, after the split of node b, we have that the shortest paths from node b to $\tilde{b}$ and vice versa both pass through nodes a and c, thus

$$Q(H) = \mathfrak{C}^{bet}(a, H_1) = \mathfrak{C}^{bet}(c, H_1) = 2 > 0 = Q(G).$$

Proposition A.7. *Consider a set $\mathcal{A} \subset \mathcal{G}$ as in (18) with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{close}(v, G)$ or $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{close}(v, G)$. Then*

1. *Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso} \cup \{\mathrm{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$.*

2. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$,*

3. *$\mathcal{A}$ satisfies Axiom 3 if and only if there is a N_0 such that $l_N \geq (1/(N-1)) \sum_{j=1}^{N-1}(1/j)$ for all $N \geq N_0$.*

4. *If $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{close}(v, G)$, then $\mathcal{A}$ satisfies Axiom 4 (and 4') if and only if $l_1 < 0$ and $l_N < 1$ for all $N \geq 2$.*

5. *If $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{close}(v, G)$, then $\mathcal{A}$ cannot satisfy Axioms 3 and 4 simultaneously. More precisely, Axiom 3 implies that Axiom 4 is violated and vice versa.*

Proof.
1. The same arguments apply as in the proof of Property C2 in Lemma 5.8.

2. By definition, we have $\mathfrak{C}_{out}^{close}(v, G), \mathfrak{C}_{in}^{close}(v, G) \geq 0$, and for every node v in an edgeless graph $\mathfrak{C}_{out}^{close}(v, G) = \mathfrak{C}_{in}^{close}(v, G) = 0$.

3. For a directed ring graph G° of size N, we have $\mathfrak{C}_{out}^{close}(v, G^\circ) = \mathfrak{C}_{in}^{close}(v, G^\circ) = (1/(N-1)) \sum_{j=1}^{N-1}(1/j)$, and therefore $Q(G^\circ) = (1/(N-1)) \sum_{j=1}^{N-1}(1/j)$ in both cases. We show that this is a lower bound for the maximal in-/out-closedness centrality of a strongly connected graph which implies 3.

   To this end, note that if $l_{vw}^G = d$ for some $d \in \{1, \cdots, |\mathcal{V}_G|-1\}$, and if $s = (v, v_1, \cdots, v_{d-1}, w)$ is a shortest path from v to w, then we have $l_{vv_i}^G = i$ for all $1 \leq i \leq d-1$ since $l_{vv_i}^G \leq i$ by definition and, moreover, if we had "$<$", then we could find a path from v to w shorter than s.

Now consider any strongly connected graph G of size N and some node $v \in \mathcal{V}_G$. Let $w \in \mathcal{V}_G \setminus \{v\}$ be a node with $l_{vw}^G \geq l_{vu}^G$ for all $u \in \mathcal{V}_G \setminus \{v\}$. Then $1 \leq l_{vw}^G \leq N-1$. Let $s = (v, v_1, \ldots, v_{d_1}, v_d)$ with $v_d = w$ be a shortest path from v to w in G. Then $\sum_{j=1}^d 1/l_{vv_j}^G = \sum_{j=1}^d (1/j)$, because $l_{vv_i}^G = i$ for all $1 \leq i \leq d$, see above. Moreover, since d is the maximal distance from v to any other node in the graph G, we have $1/l_{vu}^G \geq 1/d$ for all $u \in \mathcal{V}_G \setminus s$, thus

$$\sum_{u \in \mathcal{V}_G \setminus \{v\}} 1/l_{vu}^G \geq \sum_{j=1}^{d} \frac{1}{j} + (N-1-d)\frac{1}{d} \geq \sum_{j=1}^{N-1} \frac{1}{j}.$$

Hence, in case of the out-closeness centrality, we indeed have

$$Q(G^\circ) = \max_{v \in \mathcal{V}_{G^\circ}} \mathfrak{C}_{out}^{close}(v, G^\circ) \leq \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{close}(v, G) = Q(G).$$

The proof for the in-closeness centrality is analogous.

4. The super-spreader v^* of a directed star graph G^* of size $|\mathcal{V}_{G^*}| \geq 2$ satisfies $\mathfrak{C}_{out}^{close}(v^*, G^*) = 1$. The same applies to a star node in a bidirectional star graph. Therefore, Axioms 4 and 4' are equivalent when choosing $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{close}(v, G)$ and we obtain 4.

5. The super-spreader v^* of a directed star graph G^* of size $N \geq 2$ satisfies $\mathfrak{C}_{in}^{close}(v^*, G^*) = 0$ whereas $\mathfrak{C}_{in}^{close}(v, G^*) = 1/(N-1)$ for $v \in \mathcal{V}_{G^*} \setminus \{v^*\}$. Therefore,

$$\max_{v \in \mathcal{V}_{G^*}} \mathfrak{C}_{in}^{close}(v, G^*) = 1/(N-1) \leq (1/(N-1)) \sum_{j=1}^{N-1} (1/j) = \max_{v \in \mathcal{V}_{G^\circ}} \mathfrak{C}_{in}^{close}(v, G^\circ)$$

for all directed ring graphs G° of the same size N. Thus, recalling the proof of 3., 5. follows.

□

Corollary A.8. *Suppose that the sequence $(l_N)_{N \in \mathbb{N}}$ satisfies $l_1 < 0$, $0 \leq l_N < 1$ for all $N \geq 2$, and there is $N_0 \geq 3$ such that $l_N \geq (1/(N-1)) \sum_{j=1}^{N-1}(1/j)$ whenever $N \geq N_0$. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso} \cup \{\mathrm{id}\}$ such that $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G} | \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{close}(v, G) \leq l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 5. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

Proof. Clearly, $\mathcal{A}$ satisfies Axiom 6. For Axiom 5, consider a network G composed of two disjoint components G_1 of size $N_1 > 0$ and G_2 of size $N_2 > 0$ with $N = N_1 + N_2$. Then, for any $v \in G_i$, $i = 1, 2$, we find

$$\mathfrak{C}_{out}^{close}(v, G) = \frac{1}{N-1}(N_i - 1)\mathfrak{C}_{out}^{close}(v, G_i) < \mathfrak{C}_{out}^{close}(v, G_i).$$

Therefore, Axiom 5 is satisfied if the sequence $(l_N)_N$ is non-decreasing. The rest follows from Proposition A.7. □

Remark A.9. *Similar to the previous discussions, out-closeness and in-closeness can also be combined to form an "overall" closeness measure $\mathfrak{C}^{close}(v, G) := \frac{1}{2}\big(\mathfrak{C}_{in}^{close}(v, G) + \mathfrak{C}_{out}^{close}(v, G)\big)$. As above $\mathfrak{C}^{close}$ may be used to define a network acceptance set for pandemic cyber contagion. We leave the details to the reader.*

A.3 Betweenness Centrality

Note that centrality measures which define centrality of a node not in absolute terms but relative to the centrality of other nodes may not be suitable for this type of control. A prominent example of this is betweenness centrality $\mathfrak{C}^{bet}$:

Proposition A.10. *Consider a network acceptance set $\mathcal{A}$ as in* (18) *with $Q(G) = \max_{v\in\mathcal{V}_G} \mathfrak{C}^{bet}(v, G)$.*

1. *Let $\mathfrak{C}^{bet}$ be given as in* (17)*. If $\mathcal{A}$ satisfies Axiom 2, then Axioms 4' and Axiom 4 are violated. Conversely, if $\mathcal{A}$ satisfies Axiom 4' or Axiom 4, then Axiom 2 is violated.*

2. *Let us modify the definition in* (17) *by setting*

$$\mathfrak{C}^{bet}(v, G) = \sum_{u,w\in\mathcal{V}_G} \frac{\sigma_{uw}(v)}{\sigma_{uw}}.$$

   Then, if $\mathcal{A}$ satisfies Axiom 3, Axioms 4' and Axiom 4 are violated. Conversely, if $\mathcal{A}$ satisfies Axiom 4' or Axiom 4, then Axiom 3 is violated.

Proof. 1. If G^c is a complete graph, then there is only one shortest path between two distinct nodes $u, w \in \mathcal{V}$, namely the edge between them. Therefore, in complete graphs we have $\sigma_{uw}(v) = 0$ if $v \notin \{u, w\}$, and we thus find $\mathfrak{C}^{bet}(v, G^c) = 0$ for all $v \in \mathcal{V}_{G^c}$. Hence, $Q(G^c) = 0$. Clearly, any edge-less graph $G^\emptyset = (\mathcal{V}, \emptyset)$ also satisfies $Q(G^\emptyset) = 0$. Hence, 1. follows.

2. In this case, $\mathfrak{C}^{\mathrm{bet}}(v, G^c) = 2(N-1)$ for each node v in a complete graph G^c of size N, that is $Q(G^c) = 2(N-1)$. However, for any strongly connected network G of size N we have that for each pair of nodes $v, w \in \mathcal{V}_G$ shortest paths from v to w exist and vice versa. Thus, we always have $\sigma_{vw}(v)/\sigma_{vw} = \sigma_{wv}(v)/\sigma_{wv} = 1$, and hence, for any node $v \in \mathcal{V}_G$ we find

$$Q(G) \geq \mathfrak{C}^{bet}(v, G) \geq \sum_{w\in\mathcal{V}_G} \Big(\frac{\sigma_{vw}(v)}{\sigma_{vw}} + \frac{\sigma_{wv}(v)}{\sigma_{wv}}\Big) = 2\cdot(N-1) = Q(G^c).$$

   Now 2. follows.

□

Appendix B Undirected Networks

We denote the set of undirected networks by

$$\mathcal{G}^{ud} := \{G = (\mathcal{V}_G, \mathcal{E}_G) \in \mathcal{G} | (v, w) \in \mathcal{E}_G \Leftrightarrow (w, v) \in \mathcal{E}_G\} \subset \mathcal{G}.$$

In the following, we discuss how the presented theory in the main part of this paper would change if we restrict the domain to $\mathcal{G}^{ud}$ instead of $\mathcal{G}$. Indeed, most of the definitions and results can easily be adapted to this class of networks and we leave this to the reader apart from a few comments and additional examples which are collected in this section. Regarding the Axioms 3 and 4 presented in Section 4, note that an undirected graph is strongly connected if and only if it is weakly connected which in this case is only referred to as being connected, and that for an arbitrary graph $G \in \mathcal{G}^{ud}$, any super-spreader $v^* \in \mathcal{V}_G$ is a star node. We thus obtain the following versions of axioms 3 and 4 for undirected graphs:

- *Axiom 3^{ud}:* There exists $N_0 \in \mathbb{N}$ such that there is a connected graph in $\mathcal{A}$ of size N for all $N \geq N_0$.

- *Axiom 4^{ud}:* Any network with a star node is not acceptable.

B.1 Interventions for Undirected Networks

If we restrict the discussion to the class $\mathcal{G}^{ud}$, then any undirected graph should always be transformed into a new undirected graph. For convenience, as we view the undirected networks $\mathcal{G}^{ud}$ as a subset of the potentially directed networks $\mathcal{G}$, the following elementary interventions on undirected graphs are defined on $\mathcal{G}$, that is $\kappa : \mathcal{G} \to \mathcal{G}$, but satisfy $\kappa(\mathcal{G}^{ud}) \subset \mathcal{G}^{ud}$. Note that only those basic interventions from Section 3.1 that come with a manipulation of network edges need to be adjusted.

$\mathcal{I}^{ud}_{e\_del}$ **Edge Deletion**: *Consider a node tuple (v, w), $v, w \in \mathbb{V}$. We let*

$$\kappa^{v,w}_{e\_del} := \kappa^{(w,v)}_{e\_del} \circ \kappa^{(v,w)}_{e\_del} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \setminus \{(v, w), (w, v)\})$$

denote the deletion of the full edge between nodes v and w. Clearly, $\kappa^{v,w}_{e\_del} = \kappa^{w,v}_{e\_del}$. We set

$$\mathcal{I}^{ud}_{e\_del} := \{\kappa^{v,w}_{e\_del} \mid v, w \in \mathbb{V}\}.$$

$\mathcal{I}^{ud}_{e\_add}$ **Edge Addition**: *The addition of an edge between nodes $v, w \in \mathbb{V}$ with $v \neq w$ is given by*

$$\kappa^{v,w}_{e\_add} := \kappa^{(w,v)}_{e\_add} \circ \kappa^{(v,w)}_{e\_add} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \cup (\{(v, w), (w, v)\} \cap \mathcal{V}_G \times \mathcal{V}_G)),$$

and we let

$$\mathcal{I}^{ud}_{e\_add} := \{\kappa^{v,w}_{e\_add} \mid v, w \in \mathbb{V}\}.$$

$\mathcal{I}^{ud}_{shift}$ **Edge Shift**: *An existing full edge between v and w can be shifted to a full edge between q and r by*

$$\kappa^{\{v,w\},\{q,r\}}_{shift} := \kappa^{(w.v),(r,q)}_{shift} \circ \kappa^{(v,w),(q,r)}_{shift}.$$

Note that unlike the undirected case $G \in \mathcal{G}^{ud}$, the order of the nodes v, w and q, r is generally relevant when the intervention is applied to networks $G \in \mathcal{G}$. We set

$$\mathcal{I}^{ud}_{shift} := \{\kappa^{\{v,w\},\{q,r\}}_{shift} \mid v, w, q, r \in \mathbb{V}\}.$$

$\mathcal{I}^{ud}_{split}$ **Node Splitting**: For node splitting in undirected networks, we need to restrict to interventions from the set

$$\mathcal{I}^{ud}_{split} := \{\kappa^{\mathcal{L},v,\tilde{v}}_{split} | v, \tilde{v} \in \mathcal{V}, \mathcal{L} \subset \mathbb{E}, (q, r) \in \mathcal{L} \Leftrightarrow (r, q) \in \mathcal{L}\} \subset \mathcal{I}_{split}.$$

B.2 Examples

As in the main part of this paper we consider examples based on acceptance sets $\mathcal{A} \subset \mathcal{G}^{ud}$ of the form

$$\mathcal{A} = \{G \in \mathcal{G}^{ud} | Q(G) \leq l_{N_G}\} \tag{23}$$

where $Q : \mathcal{G}^{ud} \to \mathbb{R} \cup \{-\infty, \infty\}$. In principle, any Q from the previous discussion on directed networks can also be applied here and the results from the directed case essentially also apply to the undirected case. Only some proof or limits l_N need to be adjusted as we will see in the following.

Figure 7: A undirected tree (left), and line (right) graph, consisting of $N = 7$ nodes. Note that the line graph is a special case of a tree since it does not contain any cycles.

B.2.1 Control of the Average Total Degree

As before choosing $Q(G) = \mathbb{E}[K_G]$ in (23) does not yield a network acceptance set for cyber pandemic risk. Indeed recall Proposition 7.8 and compare to Proposition B.1 below. In this case the proof is based on *tree graphs*: a connected undirected acyclic graph $G^t \in \mathcal{G}^{ud}$ is called an *undirected tree*.

Proposition B.1. *Suppose that $\mathcal{A}$ is given by* (23) *with* $Q(G) = \mathbb{E}[K_G]$. *If Axiom* 3^{ud} *is satisfied, then Axiom* 4^{ud} *is violated, and vice versa.*

Proof. An undirected connected graph G of size N has a minimal number of edges if and only if G is an undirected tree, see Theorem 6 in [12]. One easily verifies that this minimal number equals the number of edges of an undirected line graph of size N, see Figure 7. Therefore G contains at least $2(N-1)$ directed edges. However, this also applies to the bidirectional star graph, which is a special case of a tree graph. This proves the assertion. ☐

B.2.2 Control of the Second Moment of the Total Degree Distribution

As in the directed case, we find that choosing $Q(G) = \mathbb{E}[K_G^2]$ in (23) is a suitable way to define network acceptance sets for cyber pandemic risk. For the proof, we need the following lemma:

Lemma B.2. *Fix $N \in \mathbb{N}$. The minimal second moment $Q(G^t) = \mathbb{E}[K_{G^t}^2]$ among all undirected tree graphs $G^t \in \mathcal{G}^{ud}$ of size N is attained by the undirected line graphs $L = (\mathcal{V}_L, \mathcal{E}_L)$, where for $\mathcal{V}_L = \{v_1, \cdots, v_N\} \subset \mathbb{V}$ we have $\mathcal{E}_L = \{(v_1, v_2), (v_2, v_1), \cdots (v_{N-1}, v_N), (v_N, v_{N-1})\}$.*

Proof. We prove the result by induction. First, note that for $N = 2$ and some arbitrary $v_1, v_2 \in \mathbb{V}$ the only undirected tree G^t is given by $G^t = (\{v_1, v_2\}, \{(v_1, v_2), (v_2, v_1)\})$ which is a line graph. Now, suppose that the statement holds for some $N \geq 2$, and consider a tree G^t of size $N+1$. Then G^t contains at least two nodes with a total degree of 1, called *leaves*, see Corollary 9 in [12]. Consider an enumeration of the nodes $\mathcal{V}_{G^t}$ such that v_{N+1} is a leaf of G^t with (only) neighbor v_N. Delete node v_{N+1} such that we obtain the network $H = \kappa_{n\_del}^{v_{N+1}}(G^t)$. Note that H is a tree graph of size N. Now consider the line graph L of the same size defined on the vertex set $\mathcal{V}_{G^t} \setminus \{v_{N+1}\}$ with leaf v_N. By induction hypothesis, we have

$$\mathbb{E}[K_L^2] \leq \mathbb{E}[K_H^2], \quad \text{and thus} \quad \sum_{i=1}^{N} (k_{v_i}^L)^2 \leq \sum_{i=1}^{N} (k_{v_i}^H)^2.$$

Now, let $\tilde{L} = (\mathcal{V}_{G^t}, \mathcal{E}_L \cup \{(v_N, v_{N+1}), (v_{N+1}, v_N)\})$, which is a line graph of size $N+1$. Since node v_N is a leave in L, we find $1 = k_{v_N}^L \leq k_{v_N}^H$. Moreover, $k_{v_i}^{\tilde{L}} = k_{v_i}^L$, $k_{v_i}^G = k_{v_i}^H$ for $i = 1, \cdots, N-1$, and we have $k_{v_N}^{\tilde{L}} = k_{v_N}^{L} + 1 = 2$, $k_{v_N}^{G^t} = k_{v_N}^{H} + 1 \geq 2$ (H is connected so $k_{v_N}^{H} \geq 1$), and $k_{v_{N+1}}^{G^t} = k_{v_{N+1}}^{\tilde{L}} = 1$. In total, this yields

$$\begin{aligned}\mathbb{E}[K_{\tilde{L}}^2] &= \frac{1}{N+1}\sum_{i=1}^{N+1}(k_{v_i}^{\tilde{L}})^2 = \frac{1}{N+1}\Big(\sum_{i=1}^{N-1}(k_{v_i}^{L})^2 + (k_{v_N}^{L}+1)^2 + 1^2\Big)\\ &= \frac{1}{N+1}\Big(\sum_{i=1}^{N}(k_{v_i}^{L})^2 + 4 + 1\Big) \leq \frac{1}{N+1}\Big(\sum_{i=1}^{N}(k_{v_i}^{H})^2 + (k_{v_N}^{G^t})^2 + 1\Big) = \mathbb{E}[K_{G^t}^2].\end{aligned}$$

□

Proposition B.3. *Suppose that $\mathcal{A}$ is given by* (23) *with $Q(G) = \mathbb{E}[(K_G^2]$.*

1. *Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del}^{ud} \cup \mathcal{I}_{n\_split}^{ud} \cup \{\mathrm{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$.*
2. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$,*
3. *$\mathcal{A}$ satisfies Axiom 3^{ud} if and only if there is a N_0 such that $l_N \geq 4 - 6/N$ for all $N \geq N_0$.*
4. *$\mathcal{A}$ satisfies Axiom 4^{ud} if and only if $l_N < N - 1$ for all $N \geq 1$.*

Proof. See the proof of Proposition7.13 for 1.-2 and 4. As for 3., note that we only need to consider connected networks that come with a minimal number of edges since $Q(G) = \mathbb{E}[K_G^2]$ is $\mathcal{I}_{e\_del}$-monotone according to 1, and these are the undirected tree graphs, see the proof of Proposition B.1. The second moment of total degrees is minimized among all undirected tree graphs of a fixed size N by the undirected line graphs, see Lemma B.2, and can be calculated as

$$\mathbb{E}[K_L^2] = \frac{1}{N}(2 \cdot 1 + (N-2) \cdot 4) = \frac{4N-6}{N} = 4 - \frac{6}{N}.$$

□

Corollary B.4. *Suppose that the sequence $(l_N)_{N\in\mathbb{N}}$ satisfies the constraints given by 2.–4. of Proposition B.3. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{e\_del}^{ud} \cup \mathcal{I}_{n\_split}^{ud} \cup \{\mathrm{id}\}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G}^{ud} | \mathbb{E}[(K_G)^2] \leq l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 5. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

B.2.3 Control of Epidemic Threshold

Recall the epidemic threshold of the SIR model for undirected networks given in (1). Rearranging the inequality shows that the ratio of second and first moment may be a promising candidate for the control of network contagion

$$Q(G) = \begin{cases} \frac{\mathbb{E}[K_G^2]}{\mathbb{E}[K_G]} & \text{if } \mathbb{E}[K_G] > 0 \\ 0 & \text{if } \mathbb{E}[K_G] = 0. \end{cases} \tag{24}$$

Note, however, that risk management with respect to this quantity is not completely compatible with edge deletions:

Proposition B.5. *Q as given in* (24) *is not $\mathcal{I}_{e\_del}^{ud}$-monotone.*

Proof. Suppose we delete the edges $\{(v,w),(w,v)\}$ between two adjacent nodes $v,w \in \mathcal{V}_G$ in a network G of size $N \geq 3$, and let $\tilde{G} = \kappa_{e\_del}^{v,w}(G)$. Further suppose that $\tilde{G}$ does contain edges, so that $\mathbb{E}[K_{\tilde{G}}], \mathbb{E}[K_{\tilde{G}}^2] > 0$ and thus $Q(\tilde{G}) = \mathbb{E}[K_{\tilde{G}}^2]/\mathbb{E}[K_{\tilde{G}}]$. If Q were $\mathcal{I}_{e\_del}^{ud}$-monotone, then

$$\frac{\mathbb{E}[K_G^2]}{\mathbb{E}[K_G]} - \frac{\mathbb{E}[K_{\tilde{G}}^2]}{\mathbb{E}[K_{\tilde{G}}]} \geq 0, \quad \text{i.e. } \mathbb{E}[K_{\tilde{G}}]\mathbb{E}[K_G^2] - \mathbb{E}[K_G]\mathbb{E}[K_{\tilde{G}}^2] \geq 0. \tag{25}$$

We can express the moments of $\tilde{G}$ in terms of the moments of G by

$$\mathbb{E}[K_{\tilde{G}}] = \mathbb{E}[K_G] - \frac{2}{N}, \qquad \mathbb{E}[K_{\tilde{G}}^2] = \mathbb{E}[K_G^2] + \frac{2}{N}(1 - (k_v^G + k_w^G)).$$

Therefore,

$$\begin{aligned}\mathbb{E}[K_{\tilde{G}}]\mathbb{E}[K_G^2] - \mathbb{E}[K_G]\mathbb{E}[K_{\tilde{G}}^2] &= \Big(\mathbb{E}[K_G] - \frac{2}{N}\Big)\mathbb{E}[K_G^2] - \mathbb{E}[K_G]\Big(\mathbb{E}[K_G^2] + \frac{2}{N}(1 - (k_v^G + k_w^G))\Big) \\ &= \frac{2}{N}\Big(- \mathbb{E}[K_G^2] - \mathbb{E}[K_G] + \mathbb{E}[K_G](k_v^G + k_w^G)\Big).\end{aligned}$$

Hence, (25) is satisfied if and only if $\mathbb{E}[K_G](k_v^G + k_w^G) - (\mathbb{E}[K_G^2] + \mathbb{E}[K_G]) \geq 0$, i.e., when

$$(k_v^G + k_w^G) \geq \frac{\mathbb{E}[K_G^2]}{\mathbb{E}[K_G]} + 1. \tag{26}$$

One easily constructs examples where (26) is not satisfied. $\square$

For the management of risk under edge deletions in a given network G, we thus need to restrict ourselves to those edge deletions that satisfy (26), i.e., that target edges between nodes with sufficiently large degrees.

Proposition B.6. *Let $\mathcal{A}$ be given by (23) and Q in (24). Then*

1. *Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}_{n\_split}^{ud} \cup \{\mathrm{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$.*
2. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$.*
3. *$\mathcal{A}$ satisfies Axiom 3^{ud} if and only if there is a N_0 such that $l_N \geq 2 - \frac{1}{N-1}$ for all $N \geq N_0$.*
4. *Suppose that $l_1 < 0$, $l_N < N/2$ for all $2 \leq N \leq 6$ and that $l_N < \frac{4N-1}{N+1}$ for all $N \geq 7$. Then $\mathcal{A}$ satisfies Axiom 4^{ud}.*

Proof. 1. Let $v \in \mathcal{V}_G$ be a node of the network G which is split into v and $\tilde{v}$ with a resulting network $\tilde{G}$. Again, utilizing (20) and $(N+1)\mathbb{E}[K_{\tilde{G}}] = N\mathbb{E}[K_G]$, we see that

$$\frac{\mathbb{E}[K_{\tilde{G}}^2]}{\mathbb{E}[K_{\tilde{G}}]} = \frac{\frac{1}{N+1}\Big(\sum_{w\neq v,\tilde{v}}(k_w^{\tilde{G}})^2 + (k_v^{\tilde{G}})^2 + (k_{\tilde{v}}^{\tilde{G}})^2\Big)}{\frac{1}{N+1}\Big(\sum_{w\neq v,\tilde{v}} k_w^{\tilde{G}} + k_v^{\tilde{G}} + k_{\tilde{v}}^{\tilde{G}}\Big)} \leq \frac{\sum_{w\in\mathcal{V}_G}(k_w^G)^2}{\sum_{w\in\mathcal{V}_G} k_w^G} = \frac{\mathbb{E}[K_G^2]}{\mathbb{E}[K_G]}.$$

2. is obvious.

3. For a line graph G of size $N \geq 2$, we obtain

$$Q(G) = \frac{\mathbb{E}[K_G^2]}{\mathbb{E}[K_G]} = \frac{4 - \frac{6}{N}}{2 - \frac{2}{N}} = \frac{2N-3}{N-1}.$$

We show that for any connected graph $H \in \mathcal{G}^{ud}$ of size $n \geq 2$ we have

$$Q(H) \geq \frac{2N-3}{N-1} = 2 - \frac{1}{N-1}. \tag{27}$$

To this end, consider the following three cases: If $k_v^H \geq 2$ for all $v \in \mathcal{V}_H$ it follows that $(k_v^H)^2 \geq 2k_v^H$ for all $v \in \mathcal{V}_H$ and thus

$$\mathbb{E}[K_H^2] \geq 2\mathbb{E}[K_H] \geq \left(2 - \frac{1}{N-1}\right)\mathbb{E}[K_H],$$

so (27) holds. Suppose that $k_v^H \leq 2$ for all $v \in \mathcal{V}_H$. Then H is either a undirected ring graph (i.e. $k_v^H = 2$ for all $v \in \mathcal{V}_H$) or an undirected line graph. In case of the undirected ring graph choose arbitrary $v, w \in \mathcal{V}_H$ such that $(v, w) \in \mathcal{E}_H$ (and thus also $(w, v) \in \mathcal{E}_H$). Note that v, w satisfy condition (26) in the proof of Proposition B.5, so that deleting the edges (v, w) and (w, v) decreases Q. Notice that after the deletion of those edges we are left with an undirected line graph. As a last case, suppose that there exists $v, w \in \mathcal{V}_H$ such that $k_v^H \geq 3$ and $k_w^H = 1$. Choose a neighbor $s \in \mathcal{V}_H$ of v such that

- $s \neq w$,
- s is not a neighbor of w,
- there is a path from v to w not passing through the edge (v, s).

This is possible because $k_v^H \geq 3$. Indeed, if w happens to be a neighbor of v, then choose as s any of the other neighbors of v. If w is not a neighbor of v and there is a neighbor u of v such that any path from u to w passes through the node v, then let $s = u$. Finally, if w is not a neighbor of v and all neighbors u of v allow for a path from u to w which does not pass through v, then at most one of those neighbors can be a neighbor of w ($k_w^H = 1$), so let s be one of the other neighbors. Now let $\tilde{H}$ denote the graph obtained from H by removing the edges (s, v) and (v, s) and adding the edges (s, w) and (w, s). Note that $\tilde{H}$ is connected, because any path through (v, s) or (s, v) can be redirected to a path passing through w. Then $\mathbb{E}[K_H] = \mathbb{E}[K_{\tilde{H}}]$ since we did not alter the total number of edges. However,

$$\begin{aligned}
\mathbb{E}[K_{\tilde{H}}^2] &= \frac{1}{N}\left(\sum_{\substack{u \in \mathcal{V}_H \\ u \neq v, w}} (k_u^H)^2 + (k_v^H - 1)^2 + (k_w^H + 1)^2\right) \\
&\leq \frac{1}{N}\left(\sum_{\substack{u \in \mathcal{V}_H \\ u \neq v, w}} (k_u^H)^2 + (k_v^H)^2 + (k_w^H)^2\right) = \mathbb{E}[K_H^2]
\end{aligned}$$

since $x^2 + y^2 \geq (x-1)^2 + (y+1)^2$ whenever $x - y \geq 1$. Consequently, $Q(\tilde{H}) \leq Q(H)$. If $\tilde{H}$ falls under one of the first two cases, the assertion is proved. Otherwise, $\tilde{H}$ itself falls under the third case and can again be altered accordingly, with decreasing Q, until we finally satisfy the conditions of one of the first two cases.

4. Suppose that $G \in \mathcal{G}^{ud}$ has $N \geq 2$ nodes and contains a star node $v^* \in \mathcal{V}_G$. Let $\tilde{G} = \kappa_{n\_del}^{v^*}(G)$. We estimate

$$Q(G) = \frac{\mathbb{E}\left[K_G^2\right]}{\mathbb{E}\left[K_G\right]} = \frac{N + 2\mathbb{E}\left[K_{\tilde{G}}\right] + \mathbb{E}\left[K_{\tilde{G}}^2\right]}{2 + \mathbb{E}\left[K_{\tilde{G}}\right]} \geq \frac{N + 3\mathbb{E}\left[K_{\tilde{G}}\right]}{2 + \mathbb{E}\left[K_{\tilde{G}}\right]}$$

where we used that $\mathbb{E}\left[K_H^2\right] \geq \mathbb{E}\left[K_H\right]$ for any $H \in \mathcal{G}^{ud}$ since K_H is non-negative integer valued. Note that the function $f(x) = \frac{N+3x}{2+x}$, $x > -2$, non-decreasing for $N \leq 6$ and decreasing for $N \geq 7$. Also note that $\mathbb{E}\left[K_{\tilde{G}}\right]$ ranges between 0 and $N-1$. Hence, for $N \leq 6$ we obtain that $Q(G) \geq N/2$ and for $N \geq 7$ we deduce that $Q(G) \geq (4N-1)/(N+1)$. $\square$

Note that $(4N-1)/(N+1)$ is increasing in N and larger than 3 for $N \geq 7$, so there are sequences $(l_N)_{N\in\mathbb{N}}$ simultaneously satisfying the constraints given in 3. and 4. of Proposition B.8, and, of course, also 2.

Corollary B.7. *Suppose that the sequence $(l_N)_{N\in\mathbb{N}}$ satisfies the constraints given in 2.–4. of Proposition B.6. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}^{ud}_{n\_split} \cup \{\mathrm{id}\}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G}^{ud} | \, Q(G) \leq l_{|\mathcal{V}_G|}\}$$

where Q is given in (24) is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 5. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

Proof. Clearly, $\mathcal{A}$ satisfies Axiom 6. For Axiom 5, suppose that we have two disjoint acceptable graphs G, H with size N and M, respectively, and let $l := \max\{l_N, l_M\}$. Further suppose that $\mathbb{E}[K_G] > 0$ or $\mathbb{E}[K_H] > 0$, the other case being trivial. By disjointness, we have

$$\mathbb{E}[K^2_{G\cup H}] = \frac{1}{N+M}(N\mathbb{E}[K^2_G] + M\mathbb{E}[K^2_H]), \qquad \mathbb{E}[K_{G\cup H}] = \frac{1}{N+M}(N\mathbb{E}[K_G] + M\mathbb{E}[K_H]).$$

Moreover, note that $G, H \in \mathcal{A}$ implies $\mathbb{E}[K^2_G] \leq l_N \mathbb{E}[K_G]$ and $\mathbb{E}[K^2_H] \leq l_M \mathbb{E}[K_H]$. Hence, we obtain

$$\frac{\mathbb{E}[K^2_{G\cup H}]}{\mathbb{E}[K_{G\cup H}]} = \frac{N\mathbb{E}[K^2_G] + M\mathbb{E}[K^2_H]}{N\mathbb{E}[K_G] + M\mathbb{E}[K_H]} \leq \frac{N \cdot l \cdot \mathbb{E}[K_G] + M \cdot l \cdot \mathbb{E}[K_H]}{N \cdot \mathbb{E}[K_G] + M \cdot \mathbb{E}[K_H]} = l\frac{N\mathbb{E}[K_G] + M\mathbb{E}[K_H]}{N\mathbb{E}[K_G] + M\mathbb{E}[K_H]} = l.$$

The rest follows from Proposition B.6. $\square$

B.2.4 Control of Maximal Total Node Degrees

In analogy to Proposition A.4, we obtain:

Proposition B.8. *Consider a set $\mathcal{A} \subset \mathcal{G}^{ud}$ as in (23) with $Q(G) = \max_{v\in\mathcal{V}_G} \mathfrak{C}^{deg}(v, G)$. Then*

1. *Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}^{ud}_{e\_del} \cup \mathcal{I}^{ud}_{n\_split} \cup \{\mathrm{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$.*
2. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$,*
3. *$\mathcal{A}$ satisfies Axiom 3^{ud} if and only if there is a N_0 such that $l_N \geq 2$ for all $N \geq N_0$.*
4. *$\mathcal{A}$ satisfies Axiom 4^{ud} if and only if $l_N < N - 1$ for all $N \geq 1$.*

Proof. See the proof of Proposition A.4 for 1., 2., and 4. As for 3., note that any undirected tree graph of size $N \geq 3$ contains at least one node with a total degree of at least 2, and as before the tree graphs represent the connected graphs with minimal Q in $\mathcal{G}^{ud}$ for a given network size N since $Q(G)$ is $\mathcal{I}_{e\_del}$-monotone. This shows the 'only if'-part, and for the 'if'-part consider undirected line graphs. $\square$

Corollary B.9. *Suppose that the sequence $(l_N)_{N\in\mathbb{N}}$ satisfies the constraints given by 2.-4. of Proposition B.8. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}^{ud}_{e\_del} \cup \mathcal{I}^{ud}_{n\_split} \cup \{\mathrm{id}\}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G}^{ud} | \max_{v\in\mathcal{V}_G} \mathfrak{C}^{deg}(v,G) \leq l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 5. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

B.2.5 Control of the Total Closeness Centrality

Consider the quantity $Q(G) = \max_{v\in\mathcal{V}_G} \mathfrak{C}^{close}(v,G)$ with

$$\mathfrak{C}^{close}(v,G) := \frac{1}{2}\big(\mathfrak{C}^{close}_{in}(v,G) + \mathfrak{C}^{close}_{out}(v,G)\big).$$

Proposition B.10. *Consider a set $\mathcal{A} \subset \mathcal{G}$ as in (23) with $Q(G) = \max_{v\in\mathcal{V}_G} \mathfrak{C}^{close}(v,G)$. Then*

1. *Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}^{ud}_{e\_del} \cup \mathcal{I}^{ud}_{s\_iso} \cup \{\mathrm{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\mathrm{id}\} \subsetneqq \mathcal{I}^{\downarrow}$.*
2. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$,*
3. *$\mathcal{A}$ satisfies Axiom 3^{ud} if and only if there is a N_0 such that $l_N \geq (1/(N-1)) \sum_{j=1}^{(N-1)/2}(2/j)$ for all $N \geq N_0$ which are odd, and $l_N \geq (1/(N-1))\big(\sum_{j=1}^{(N-2)/2}(2/j) + 2/N\big)$ for all $N \geq N_0$ which are even.*
4. *$\mathcal{A}$ satisfies Axiom 4^{ud} if and only if $l_1 < 0$ and $l_N < 1$ for all $N \geq 2$.*

Proof. See the proof of Proposition A.7 for 1. and 2. For 4., note that the star node v^* in a bidirectional star graph G^* of size $|\mathcal{V}_{G^*}| \geq 2$ comes with $\mathfrak{C}^{close}_{in}(v^*,G^*) = \mathfrak{C}^{close}_{out}(v^*,G^*) = 1$, and thus $Q(G^*) = 1$.

Regarding 3., it suffices again to restrict the discussion to tree graphs since Q is $\mathcal{I}_{e\_del}$-monotone. Consider a tree graph G^t of size N, and let $v, w \in \mathcal{V}_{G^t}$ be two nodes (not necessarily unique) that come with a maximal distance $l^{G^t}_{vw} (= l^{G^t}_{wv}) \leq N-1$ among all node pairs. Moreover, note that the path $p^{G^t}_{vw} := (v, v_2, \cdots, w)$ connecting v and w in G^t is unique since a tree graph contains no cycles. Now we distinguish between two cases:

1. Suppose $l^{G^t}_{vw}$ is even. Then the number of nodes on the path $p^{G^t}_{vw}$ is odd. Thus we find a node $u \in p^{G^t}_{vw}$ that lies in the center of the path connecting v and w, coming with $l^{G^t}_{vu} (= l^{G^t}_{uv}) = l^{G^t}_{wu} (= l^{G^t}_{uw}) = l^{G^t}_{vw}/2$. Moreover, since v and w come with the maximal distance among all node pairs, we have $l^{G^t}_{uq} \leq l^{G^t}_{vw}/2$ for all nodes $q \in \mathcal{V}_{G^t}$:
    a) The statement is clear for each node q that lies on the path connecting v and w.
    b) Suppose the path $p^{G^t}_{vq}$ between q and v or $p^{G^t}_{wq}$ between q and w does not intersect with the path $p^{G^t}_{vw}$ connecting v and w (apart from the node v). W.l.o.g. assume $p^{G^t}_{vq} \setminus \{v\} \cap p^{G^t}_{vw} = \emptyset$. Since all node pairs in G^t are connected by exactly one path due to the absence of cycles in G^t, we thus have $l^{G^t}_{wq} = l^{G^t}_{vw} + l^{G^t}_{vq} > l^{G^t}_{vw}$. But this contradicts the assumption that v and w come with the maximal distance among all node pairs.
    c) For the last case, consider the possibility that the paths connecting node q to v and to w depart from a node $r \in p^{G^t}_{vw}$. Then $l^{G^t}_{vq} = l^{G^t}_{vr} + l^{G^t}_{rq}$ and $l^{G^t}_{wq} = l^{G^t}_{wr} + l^{G^t}_{rq}$. We can now either have $r = u$, or if not, then for either v or w, namely the node with a larger

distance to q, u must lie on the path connecting v and q, or w and q, respectively. If we had the case that $l^{G^t}_{uq} > l^{G^t}_{vw}/2$, then again, since G^t contains no cycles, the path between v and q or between w and q now must be larger than $l^{G^t}_{vw}$, contradicting our initial assumption.

Now, since u lies in the centre of the path between v and w, for any distance $j \leq l^{G^t}_{vw}/2$, we find two different nodes x, y on the path $p^{G^t}_{vw}$ with $l^{G^t}_{ux}, l^{G^t}_{uy} = j$. Moreover, due to $l^{G^t}_{uq} \leq l^{G^t}_{vw}/2$ for all $q \in \mathcal{V}_{G^t}$ we obtain

$$\sum_{q\in\mathcal{V}_{G^t}\setminus\{u\}} \frac{1}{l^{G^t}_{uq}} \geq \sum_{j=1}^{l^{G^t}_{vw}/2} 2\cdot\frac{1}{j} + \sum_{q\notin p^{G^t}_{vw}} \frac{1}{l^{G^t}_{vw}/2} = \sum_{j=1}^{l^{G^t}_{vw}/2} 2\cdot\frac{1}{j} + (N - l^{G^t}_{vw} - 1)\cdot\frac{1}{l^{G^t}_{vw}/2}$$

If N is odd, then $N - l^{G^t}_{vw} - 1$ is even, and because of $l^{G^t}_{vw} \leq N-1$ we then we find

$$\sum_{q\in\mathcal{V}_{G^t}\setminus\{u\}} \frac{1}{l^{G^t}_{uq}} \geq \sum_{j=1}^{(N-1)/2} 2\cdot\frac{1}{j}.$$

In the case that N is even, we find that $N - l^{G^t}_{vw} - 1$ is odd, thus

$$\sum_{q\in\mathcal{V}_{G^t}\setminus\{u\}} \frac{1}{l^{G^t}_{uq}} \geq \sum_{j=1}^{(N-2)/2} 2\cdot\frac{1}{j} + \frac{1}{l^{G^t}_{vw}/2} \geq \sum_{j=1}^{(N-2)/2} 2\cdot\frac{1}{j} + \frac{2}{N-1} \geq \sum_{j=1}^{(N-2)/2} 2\cdot\frac{1}{j} + \frac{2}{N}.$$

2. Suppose that $l^{G^t}_{vw}$ is odd. Then we find two nodes u_v and u_w in the center of the path between v and w, where $l^{G^t}_{vu_v}, l^{G^t}_{wu_w} = (l_{vw}-1)/2$, and $l^{G^t}_{wu_v}, l^{G^t}_{vu_w} = (l_{vw}+1)/2$. Moreover, analogously to the considerations from 1., we then find that $l^{G^t}_{u_vq}, l^{G^t}_{u_wq} \leq (l^{G^t}_{vw}+1)/2 \leq N/2$ for all nodes $q \in \mathcal{V}_{G^t}$. Thus, for $u \in \{u_v, u_w\}$ we have

$$\sum_{q\in\mathcal{V}_{G^t}\setminus\{u\}} \frac{1}{l^{G^t}_{uq}} = \sum_{j=1}^{(l^{G^t}_{vw}-1)/2} 2\cdot\frac{1}{j} + \frac{1}{(l^{G^t}_{vw}+1)/2} + \sum_{q\notin p^{G^t}_{vw}} \frac{1}{l^{G^t}_{uq}} \geq \sum_{j=1}^{(l^{G^t}_{vw}-1)/2} \frac{2}{j} + (N - l^{G^t}_{vw})\cdot\frac{1}{(l^{G^t}_{vw}+1)/2}.$$

Now, if N is odd, then we must have $l^{G^t}_{u_vq}, l^{G^t}_{u_wq} \leq (l^{G^t}_{vw}+1)/2 \leq (N-1)/2$, and $N - l^{G^t}_{vw}$ is even, which together yields

$$\sum_{q\in\mathcal{V}_{G^t}\setminus\{u\}} \frac{1}{l^{G^t}_{uq}} \geq \sum_{j=1}^{(N-1)/2} \frac{2}{j}.$$

If N is even, then $N - l^{G^t}_{vw}$ is odd, and therefore, we can estimate

$$\sum_{q\in\mathcal{V}_{G^t}\setminus\{u\}} \frac{1}{l^{G^t}_{uq}} \geq \sum_{j=1}^{(N-1)/2} \frac{2}{j} + \frac{1}{N/2} = \sum_{j=1}^{(N-1)/2} \frac{2}{j} + \frac{2}{N}.$$

Finally, for the line graph of size N we indeed have

$$\sum_{q\in\mathcal{V}_{L}\setminus\{u\}} \frac{1}{l^{L}_{uq}} = \sum_{j=1}^{(N-1)/2} \frac{2}{j}$$

if N is odd (which then is equivalent to l^L_{vw} being even). In the case that N is even (and thus l^L_{vw} is odd), then

$$\sum_{q\in\mathcal{V}_{L}\setminus\{u\}} \frac{1}{l^{L}_{uq}} = \sum_{j=1}^{(N-1)/2} \frac{2}{j} + \frac{2}{N}.$$

□

Corollary B.11. *Suppose that the sequence* $(l_N)_{N\in\mathbb{N}}$ *satisfies* $l_1 < 0$, $0 \le l_N < 1$ *for all* $N \ge 2$, *and there is* $N_0 \ge 3$ *such that* $l_N \ge (1/(N-1))\sum_{j=1}^{N-1}(1/j)$ *whenever* $N \ge N_0$*. Further suppose* $\mathcal{I}^{\downarrow} \subset \mathcal{I}^{ud}_{e\_del} \cup \mathcal{I}^{ud}_{s\_iso} \cup \{\mathrm{id}\}$ *such that* $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$*. Then*

$$\mathcal{A} = \{G \in \mathcal{G} | \max_{v\in\mathcal{V}_G} \mathfrak{C}^{close}(v, G) \le l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ *satisfies Axiom 1 with* $\mathcal{I}^{\downarrow}$*. Moreover, if* $\mathbb{N} \ni N \mapsto l_N$ *is non-decreasing, then* $\mathcal{A}$ *also satisfies Axiom 5. Letting* $\mathcal{C}$ *be any cost function for* $(\mathcal{A}, \mathcal{I}^{\downarrow})$*, then* $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ *is a measure of resilience to cyber contagion.*

B.2.6 Control of the Spectral Radius of Undirected Graphs

Dynamic systems on networks are usually described by operators that depend on the adjacency matrix A_G of the graph G. The linear analysis of steady states and stability properties of these states typically leads to an analysis of the spectral properties of the adjacency matrix. Of particular importance here is the largest eigenvalue λ_1^G of A_G, called the *spectral radius* of G. For details, we refer to Section 17.4 in [56].

Example B.12. *A commonly applied model for the propagation of contagious threats in cyber networks is the SIS (*Susceptible-Infected-Susceptible*) Markov process, see Section 3.2 in [6]. The single node infection dynamics of the system can be described by a set of ordinary differential equations, according to Kolmogorov's forward equation. A major problem as regards the solvability of this system of ordinary differential equations is the fact that this system is not closed as higher order moments appear, cascading up to the network size. A simplified model can be obtained when assuming that all infection probabilities in the network are pairwise uncorrelated. Given a network* G *of size* N *with enumerated nodes, this so-called* NIMFA approximation *or* individual-based model *is governed by the set of equations*

$$\frac{d\mathbb{E}[I_i(t)]}{dt} = \tau\Big(\sum_{j=1}^{N} A_G(i,j)(1 - \mathbb{E}[I_i(t)])\mathbb{E}[I_j(t)]\Big) - \gamma\mathbb{E}[I_i(t)], \quad i = 1, \dots, N, \tag{28}$$

where $\tau, \gamma > 0$ *are the infection and recovery rates, and* $I_i(t) = 1$ *if node* v_i *is infected at time* t*, and* $I_i(t) = 0$ *if node* v_i *is susceptible at time* t*. The infection probabilities of this model provide upper bounds for the actual infection probabilities and can therefore be used for a conservative estimation, see Theorem 3.3 in [50]. The stability of steady states of system* (28)*, in particular of the disease-free state* $(I_1, \cdots, I_N) = (0, \cdots, 0)$*, is now relevant in the analysis of the epidemic vulnerability of the network* G*. Linearizing the individual-based model from* (28) *around the disease-free state induces the eigenvalue problem*

$$\det(\tau A_G - \gamma\mathbb{I}_N - \lambda\mathbb{I}_N) = 0$$

where $\mathbb{I}_N$ *is the* N*-dimensional identity matrix and the largest eigenvalue of* $\tau A_G - \gamma\mathbb{I}_N$ *is given by* $\tau\lambda_1^G - \gamma$*. If* G *is undirected and connected, it can be shown that if* $\tau/\gamma < 1/\lambda_1^G$*, then the disease free state is stable and no endemic state exists; if* $\tau/\gamma > 1/\lambda_1^G$*, then the disease-free state is unstable and there exists a unique endemic state, which is stable. For details, we refer to Section 3.4.4 in [50].*

In the setting of directed graphs, however, the information of the graph spectrum may have little or no relevance in terms of graph vulnerability. For example, the only element in the spectrum of both the edgeless and the directed star graph is zero. Consequently, Axiom 2 and 4' cannot jointly be satisfied in a directed graph setting when choosing $Q(G) = \lambda_1^G$. Moreover, the spectrum of directed graphs can be complex due to the lack of the adjacency matrix' symmetry.

The following definition is needed for the proof of the next proposition:

Definition B.13. *Given a graph $G \in \mathcal{G}^{ud}$ and two nodes $v, u \in \mathcal{V}_G$, a Kelmans operation in G is a $\mathcal{I}_{shift}$-strategy where each bidirectional edge $\{(v,w),(w,v)\} \in \mathcal{E}_G$ is replaced by $\{(u,w),(w,u)\}$ if $w \neq u$ and $\{(u,w),(w,u)\} \cap \mathcal{E}_G = \emptyset$.*

Proposition B.14. *Consider a network acceptance set $\mathcal{A}$ as in (23) with $Q(G) = \lambda_1^G$. Then*

1. *Q is $\mathcal{I}^{\downarrow}$-monotone for any $\mathcal{I}^{\downarrow} \subset \mathcal{I}^{ud}_{e\_del} \cup \mathcal{I}^{ud}_{n\_split} \cup \{\mathrm{id}\}$. Hence $\mathcal{A}$ satisfies Axiom 1 with any such $\mathcal{I}^{\downarrow}$ such that $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$.*
2. *$\mathcal{A}$ satisfies Axiom 2 if and only if $l_N \geq 0$ for all $N \geq 2$,*
3. *$\mathcal{A}$ satisfies Axiom 3 if and only if there is a N_0 such that $l_N \geq \max_{j\in\{1,\cdots,N\}} \cos(\pi j/(N+1))$ for all $N \geq N_0$. In particular, this is the case if there is a N_0 such that $l_N \geq 2$ for all $N \geq N_0$.*
4. *$\mathcal{A}$ satisfies Axiom 4 if and only if $l_N < \sqrt{(N-1)}$ for all $N \geq 1$.*

Proof.

1. The spectral radius is non-increasing under edge deletions, see [15, Proposition 3.1.1]. Standard results also imply that Q is non-increasing under node splits: Let $G \in \mathcal{G}^{ud}$, and $H = \kappa^{\mathcal{J},v,\tilde{v}}_{split}(G)$ a network resulting from a split of node v by adding a new node $\tilde{v}$ and rewiring edges contained in $\mathcal{J}$, where $(v,w) \in \mathcal{J} \Leftrightarrow (w,v) \in \mathcal{J}$. Then we can construct a new graph H' from H by a consecutive edge shift where all edges $(\tilde{v}, w)$ are replaced by (v,w) and all $(w,\tilde{v})$ by (w,v). This is a particular example of a Kelmans operation, see Section 3.1.3 in [15] for details, since $\mathcal{N}_v^H \cap \mathcal{N}_{\tilde{v}}^H = \emptyset$. Note that $H' = G\dot{\cup}(\{\tilde{v}\},\emptyset)$ is a disjoint union of G and the isolated node $\tilde{v}$. Therefore, we have $\lambda_1^{H'} = \lambda_1^G$, and the spectral radius of a graph is non-decreasing under a Kelmans operation, see [15, Proposition 3.1.5]. This gives $\lambda_1^H \leq \lambda_1^{H'} = \lambda_1^G$.
2. trivial
3. Note that undirected line graphs of size N have a minimal spectral radius among all connected graphs of this size in $\mathcal{G}^{ud}$, cf. [63, Theorem 1]. Their spectrum consists of the eigenvalues $\lambda_j = 2\cos(\pi j/(N+1))$, $j = 1, \cdots, N$, see [15, Section 1.4.4].
4. For an undirected star graph of size N, simple calculations show that the spectrum consists of the eigenvalues $\sqrt{N-1}$ and $-\sqrt{N-1}$, both with a multiplicity of one, and the eigenvalue 0 with multiplicity of $N-2$.

□

Corollary B.15. *Suppose that the sequence $(l_N)_{N\in\mathbb{N}}$ satisfies $l_1 < 0$, $0 \leq l_N < \sqrt{N-1}$ for all $N \geq 2$, and there is $N_0 \geq 4$ such that $l_N \geq 2$ whenever $N \geq N_0$. Further suppose $\mathcal{I}^{\downarrow} \subset \mathcal{I}^{ud}_{e\_del} \cup \mathcal{I}^{ud}_{n\_split} \cup \{\mathrm{id}\}$ such that $\{\mathrm{id}\} \subsetneq \mathcal{I}^{\downarrow}$. Then*

$$\mathcal{A} = \{G \in \mathcal{G}^{ud} | \lambda_1^G \leq l_{|\mathcal{V}_G|}\}$$

is a topologically invariant network acceptance set for pandemic cyber contagion where $\mathcal{A}$ satisfies Axiom 1 with $\mathcal{I}^{\downarrow}$. Moreover, if $\mathbb{N} \ni N \mapsto l_N$ is non-decreasing, then $\mathcal{A}$ also satisfies Axiom 6. Letting $\mathcal{C}$ be any cost function for $(\mathcal{A}, \mathcal{I}^{\downarrow})$, then $(\mathcal{A}, \mathcal{I}^{\downarrow}, \mathcal{C})$ is a measure of resilience to cyber contagion.

Proof. This follows from the results in Proposition B.14 noting that $\max_{j\in\{1,\cdots,N\}} 2\cos(\pi j/(N+1)) \leq 2$. Hence, Axiom 3 is satisfied whenever there is N_0 such that $l_N \geq 2$ for $N \geq N_0$. Recalling 4. of Proposition B.14 we observe that we must have $N_0 \geq 4$, and indeed note that every undirected line graph of size $N \leq 3$ is also an undirected star graph. Regarding Axiom 5, the spectrum of a disjoint union graph $G \cup H$ equals the union of the spectra of G and H, which yields $\lambda_1^{G\cup H} = \max\{\lambda_1^G, \lambda_1^H\}$. Hence, if G and H are acceptable, then the same applies to $G \cup H$ whenever the sequence $(l_N)_{N\in\mathbb{N}}$ is non-decreasing. Moreover, $\mathcal{A}$ is topologically invariant since, clearly, any two isomorphic graphs share the same graph spectrum. □

References

[1] Amini, H., Cont, R., & Minca, A. (2016). Resilience to contagion in financial networks. *Mathematical Finance*, *26*(2), 329–365.

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

[3] Armenti, Y., Crépey, S., Drapeau, S., & Papapantoleon, A. (2018). Multivariate shortfall risk allocation and systemic risk. *SIAM Journal on Financial Mathematics*, *9*(1), 90–126.

[4] Artzner, P., Delbaen, F., Eber, J.-M., & Heath, D. (1999). Coherent measures of risk. *Mathematical Finance*, *9*(3), 203–228.

[5] 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.*

[6] Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2023). Modeling and pricing cyber insurance: Idiosyncratic, systematic, and systemic risks. *European Actuarial Journal*, *13*, 1–53.

[7] Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D., & Williams, J. (2017). Contagion in cyber security attacks. *Journal of the Operational Research Society*, *68*, 780–791.

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

[9] Barrat, A., Barthélemy, M., & Vespignani, A. (2008). *Dynamical processes on complex networks.* Cambridge University Press.

[10] Bessy-Roland, Y., Boumezoued, A., & Hillairet, C. (2021). Multivariate hawkes process for cyber insurance. *Annals of Actuarial Science*, *15*, 14–39.

[11] Biagini, F., Fouque, J.-P., Frittelli, M., & Meyer-Brandis, T. (2019). A unified approach to systemic risk measures via acceptance sets. *Mathematical Finance*, *29*(1), 329–367.

[12] Bollobás, B. (1998). *Modern graph theory.* Springer.

[13] Boumezoued, A., Cherkaoui, Y., & Hillairet, C. (2023). *Cyber risk modeling using a two-phase hawkes process with external excitation* (Working Paper).

[14] Brauchle, J.-P., Göbel, M., Seiler, J., & von Busekist, C. (2020). *Cyber mapping the financial system.* Carnegie Endowment for International Peace.

[15] Brouwer, A. E., & Haemers, W. H. (2012). *Spectra of graphs.* Berlin: Springer.

[16] Cassidy, A., Feinstein, Z., & Nehorai, A. (2016). Risk measures for power failures in transmission systems. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *26*(11), 113110.

[17] Chen, C., Iyengar, G., & Moallemi, C. C. (2013). An axiomatic approach to systemic risk. *Management Science*, *59*(6), 1373–1388.

[18] 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.

[19] Chiaradonna, S., Jevtić, P., & Lanchier, N. (2023). Framework for cyber risk loss distribution of hospital infrastructure: Bond percolation on mixed random graphs approach. *Risk Analysis.*

[20] Dacorogna, M., Debbabi, N., & Kratz, M. (2023). Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *European Journal of Operational Research*, *311*(2), 708–729.

[21] Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal.*

[22] Detering, N., Mayer-Brandis, T., Panagiotou, K., & Ritter, D. (2019). Systemic risk in networks. *Network Science. An Aerial View*, 59–77.

[23] Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (eu) no 910/2014 and directive (eu) 2018/1972, and repealing directive (eu) 2016/1148 (nis 2 directive) (text with eea relevance). (2022). *European Union.*

[24] Eisenbach, T. M., Kovner, A., & Lee, M. J. (2021). *Cyber risk and the u.s. financial system: A pre-mortem analysis* (tech. rep. No. 909). Federal Reserve Bank of New York.

[25] Eisenberg, L., & Noe, T. H. (2001). Systemic risk in financial systems. *Management Science*, *47*(2), 236–249.

[26] Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal*, 1–31.

[27] ESRB (Ed.). (2020). *Systemic cyber risk.*

[28] ESRB (Ed.). (2022). *Mitigating systemic cyber risk.*

[29] Estrada, E., Hatano, N., & Benzi, M. (2012). The physics of communicability in complex networks. *Physics Reports*, *514*(3), 89–119.

[30] Fadina, T., Liu, Y., & Wang, R. (2023). A framework for measures of risk under uncertainty.

[31] Fahrenwaldt, M., 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.

[32] Feinstein, Z., Kleiber, M., & Weber, S. (2023). *Acceptable designs of traffic networks: Stochastic cell transmission models and systemic risk* (Working Paper).

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

[34] Föllmer, H. (2014). Spatial risk measures and their local specification: The locally law-invariant case. *Statistics & Risk Modeling*, *31*(1), 79–101.

[35] Föllmer, H., & Klüppelberg, C. (2014). Spatial risk measures: Local specification and boundary risk. In D. Crisan, B. Hambly, & T. Zariphopoulou (Eds.), *Stochastic analysis and applications 2014* (pp. 307–326). Springer International Publishing.

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

[37] Föllmer, H., & Weber, S. (2015). The axiomatic approach to risk measures for capital determination. *Annual Review of Financial Economics*, *7*(1), 301–337.

[38] Forscey, D., Bateman, J., Beecroft, N., & Woods, B. (2022). *Systemic cyber risk: A primer.* Carnegie Endowment for International Peace and the Aspen Institute.

[39] Fouque, J.-P., & Langsam, J. A. (Eds.). (2013). *Handbook on systemic risk.* Cambridge University Press.

[40] Gandy, A., & Veraart, L. A. M. (2017). A bayesian methodology for systemic risk assessment in financial networks. *Management Science*, *63*(12), 4428–4446.

[41] Girvan, M., & Newman, M. (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.

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

[43] 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.

[44] Hillairet, C., Réveillac, A., & Rosenbaum, M. (2023). An expansion formula for hawkes processes and application to cyber-insurance derivatives. *Stochastic Processes and their Applications*, *160*, 89–119.

[45] Hoffmann, H., Meyer-Brandis, T., & Svindland, G. (2016). Risk-consistent conditional systemic risk measures. *Stochastic Processes and their Applications*, *126*(7), 2014–2037.

[46] Hoffmann, H., Meyer-Brandis, T., & Svindland, G. (2018). Strongly consistent multivariate conditional risk measures. *Mathematics and Financial Economics*, *12*, 413–444.

[47] Hurd, T. R. (2016). *Contagion! systemic risk in financial networks*. Springer.

[48] Jackson, M. O., & Pernoud, A. (2021). Systemic risk in financial networks: A survey. *Annual Review of Economics*, *13*(1), 171–202.

[49] 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.

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

[51] Kitsak, M., Ganin, A., Elmokashfi, A., Cui, H., Eisenberg, D. A., Alderson, D. L., Korkin, D., & Linkov, I. (2023). Finding shortest and nearly shortest path nodes in large substantially incomplete networks by hyperbolic mapping. *Nature Communications*, *14*(186).

[52] Latora, V., & Marchiori, M. (2001). Efficient behavior of small-world networks. *Phys. Rev. Lett.*, *87*, 198701.

[53] Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*.

[54] Molloy, M., & Reed, B. (1995). A critical point for random graphs with a given degree sequence. *Random Structures & Algorithms*, *6*(2-3), 161–180.

[55] *National control and cyber resilience to safeguard national security. as open as possible, as secure as necessary* (tech. rep. Meld. St. 9). (2022-2023).

[56] Newman, M. (2018). *Networks: Second edition*. Oxford University Press.

[57] Pastor-Satorras, R., Castellano, C., Van Mieghem, P., & Vespignani, A. (2015). Epidemic processes in complex networks. *Reviews of Modern Physics*, *87*, 925–979.

[58] Price, D. d. S. (1965). Networks of scientific papers. *Science*, *149*(3683), 510–515.

[59] 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.

[60] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture*. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD.

[61] Salomon, J., Broggi, M., Kruse, S., Weber, S., & Beer, M. (2020). Resilience Decision-Making for Complex Systems. *ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg*, *6*(2), 020901.

[62] Song, C., Havlin, S., & Makse, H. A. (2005). Self-similarity of complex networks. *Nature*, *433*, 392–395.

[63] van Dam, E., & Kooij, R. (2007). The minimal spectral radius of graphs with a given diameter. *Linear Algebra and its Applications*, *423*(2), 408–419.

[64] Welburn, J. W., & Strong, A. M. (2022). Systemic cyber risk and aggregate impacts. *Risk Analysis*, *42*(8), 1606–1622.

[65] Xu, M., & Hua, L. (2019). Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal*, *23*(2), 220–249.

[66] Zeller, G., & Scherer, M. (2021). A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*, 1–53.

[67] Zeller, G., & Scherer, M. (2023a). *Is accumulation risk in cyber systematically underestimated?* (Working Paper).

[68] Zeller, G., & Scherer, M. (2023b). Risk mitigation services in cyber insurance: Optimal contract design and price structure. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *48*, 502–547.