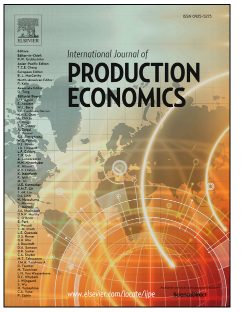
Journal Pre-proof



Exploring supply chain network resilience in the presence of the ripple effect

Yuhong Li, Christopher W. Zobel

PII: S0925-5273(20)30084-0

DOI: https://doi.org/10.1016/j.ijpe.2020.107693

Reference: PROECO 107693

To appear in: *International Journal of Production Economics*

Received Date: 27 June 2019

Revised Date: 21 February 2020

Accepted Date: 21 February 2020

Please cite this article as: Li, Y., Zobel, C.W., Exploring supply chain network resilience in the presence of the ripple effect, *International Journal of Production Economics* (2020), doi: https://doi.org/10.1016/j.ijpe.2020.107693.

Credit Author Statement

Yuhong li: Conceptualization, Methodology, Formal Analysis, Writing – Original Draft, review and editing

Christopher Zobel: Conceptualization, Methodology, Formal Analysis, Writing –review and editing

Exploring Supply Chain Network Resilience in the Presence of Ripple Effect

Yuhong Li *

Dept. of Information Technology and Decision Sciences, Old Dominion University, Norfolk, VA 23529, United States

Christopher W. Zobel [1],

Dept. of Business Information Technology, Virginia Polytechnic Institute and State University, 1007 Pamplin Hall, Blacksburg, VA 24061, United States

* Corresponding author. Email:y9li@odu.edu. Tel: +1 757 693 3110

[1] Email: czobel@vt.edu. Tel: +1 540 231 1856

Exploring Supply Chain Network Resilience in the Presence of the Ripple Effect

Abstract

This study aims to investigate overall supply chain network resilience (SCNR) in the presence of ripple effect, or risk propagation, i.e. the phenomenon that disruptions at a few firms in a supply chain network (SCN) can spread to their neighboring firms, then eventually spread to other firms in the SCN. We begin by developing a multi-dimensional quantitative framework to measure SCNR, which includes three resilience dimensions based on three different network performance indicators. Given this framework, we then systematically explore the determining factors of SCNR and present a comprehensive analysis of how network structure and node risk capacity influence different aspects of SCNR. Our results clearly indicate the following important implications for managers. First, the influence of network type on SCNR tends to be more significant in the short-term than it is in the longer-term, given the ripple effect. Second, SCNR can be improved more effectively by enhancing node risk capacity than by adjusting network structure. Third, tradeoffs exist between the robustness of the network against a disruption and its ability to recover from that disruption. Fourth, different network performance indicators can provide different perspectives on SCNR. Together these help show that the multi-dimensional framework enables a better characterization of the complexity of SCNR, and thus that it provides support for more informed managerial decision-making about investing in improving resilience. The paper concludes the discussion by addressing opportunities for further extending the research effort.

Keywords: Supply chain network resilience; risk propagation; network structure; node risk capacity

1. Introduction

Modern supply chains are complex networks that are exposed to supply chain disruptions, which are operational shutdowns directly or indirectly caused by various risks such as natural disasters, political and economic factors, labor strikes, and material shortages (Bode and Wagner 2015; Craighead et al. 2007; Scheibe and Blackhurst 2017). A supply chain network (SCN) is vulnerable to disruptions not only because of the direct impacts of those disruptions, but also because of the ripple effect (also known as risk propagation) - the phenomenon that a sudden disruption at a few nodes in a SCN can spread to neighboring nodes, and eventually adversely impact other firms (Dolgui, Ivanov, and Sokolov 2018;

Scheibe and Blackhurst 2017; Li et al. 2019). The consequence of what is initially a local disruption can thus be substantial and long-lasting.

As an example of this behavior, the hard disk drive (HDD) manufacturer Western Digital, which has a number of local factories in Thailand, suffered a 50% slump in HDD sales in the last quarter of 2011 because of major flooding in that country. These losses then affected a number of other firms within its extended supply chain. One of these firms was Hewlett Packard, a customer of Western Digital, which subsequently reported a 7% drop in revenues and blamed the HDD shortage for more than half of this decline (HP 2011). Intel, a supplier for HP, also posted a decrease in 4th Quarter revenues of $346 million as a result of lower demand following the flood (Intel 2011). Such results are common, as indicated by a recent study showing that 42% of supply chain disruptions originate below the tier one suppliers (Business Continuity Institute 2013).

Both the inherent complexity of supply chain networks and the associated effects of dynamic risk propagation make disruptions difficult to predict and manage. For example, to what extent will a strike in Shenzhen eventually influence HP's production? When will Ford's production be impacted after an earthquake in Japan? The unavoidable and unpredictable nature of such disruptions (Ponomarov and Holcomb 2009; Pettit, Croxton, and Fiksel 2013; Scheibe and Blackhurst 2017) requires a successful supply chain to have the ability to resist the impact of unanticipated disruptions and to quickly recover from them (Pettit, Fiksel, and Croxton 2010; Pettit, Croxton, and Fiksel 2013; Brusset and Teller 2017). This has led to widespread interest in supply chain resilience (SCR) – the capability of a supply chain to prepare for, to respond to, and to recover from a disruption (Jüttner and Maklan 2011; Pettit, Fiksel, and Croxton 2010; Ponomarov and Holcomb 2009).

Supply chain resilience, as a concept, can be studied from a number of different perspectives, and we focus here on measuring the resilience of the overall supply chain network (Borgatti and Li, 2009), i.e., supply chain network resilience (SCNR). By characterizing the resilience of the network as a whole, we may provide each firm inside the network with an indication of the systematic risk in their business environment (Wu, Blackhurst, and O'Grady 2007; Blackhurst, Dunn, and Craighead 2011). This improved understanding of the environment should allow these firms to prepare more effectively for potential disruptions.

In practice, building resilience involves making various resource allocation decisions based on a limited budget. Such resilience investments include, but are not limited to, activities such as increasing safety stock, contracting with multiple suppliers, optimizing network structures, establishing supplier development programs, and increasing supply chain visibility (Ivanov 2018a). Some types of investments, such as adding a new node to the network for additional warehouse capacity, may be most effective for resisting the initial impacts of a disruption, while other types of investments, such as adding temporary links to represent contracts with alternate suppliers, may be more appropriate for addressing longer-lasting impacts. In order to determine the most appropriate types of investment, therefore, it is important to understand different aspects of resilient behavior in the face of unexpected disruptions (Simchi-Levi et al. 2015).

Although the practical and theoretical importance of investigating SCNR is well-recognized, recent studies fall short in two ways: The first is that such studies mainly focus on SCNR in the context of robustness – the ability of a supply chain to maintain functionality during a disruption (Brandon-Jones et al. 2014). Robustness is often measured in terms of the ability to resist the immediate impacts of a disruption (Kim, Chen, and Linderman 2015; Zhao et al. 2011), with little emphasis being placed on longer-lasting impacts due to the ripple effect (Basole and Bellamy 2014; Dolgui, Ivanov, and Sokolov 2018). It is common, however, for local disruptions to cause significant and lengthy impacts across a SCN. For example, a major fire experienced by Meridian Magnesium Products in 2018 impacted its ability to provide necessary parts and resulted in subsequent production impacts at Fiat Chrysler, GM, Daimler, BMW, and Ford (White and Lienert 2018). This clearly shows that underestimating the effects of risk propagation can lead to misunderstanding a disruption’s potential impacts and result in less effective decision-making. We are thus motivated to investigate SCNR considering risk propagation, in order to fill this literature gap.

The second way in which recent studies also tend to fall short is that they fail to take a comprehensive and systemic view of SCNR and its determining factors. SCNR is dependent on many factors, such as disruption severity – the severity of initial disruption impact (Craighead et al. 2007; Li et al. 2019), supply chain network structure – the interconnectivity pattern among firms inside the SCN (Basole and Bellamy 2014; Kim et al. 2011), and node risk capacity – the individual firm's capability to against a potential disruption and to recover from an existing disruption (Li et al. 2019). Recent studies, however, typically focus only on specific aspects of SCNR, such as the interaction between network structure and different mitigation strategies (Basole and Bellamy 2014; Mari, Lee, and Memon 2015), rather than considering network behavior more holistically. Although these studies provide valuable insights, practical application of these insights could benefit from a broader, more comprehensive understanding of SCNR. For example, if one were able to increase SCNR both by improving a firm's inherent recoverability from a disruption and by improving network structure through establishing additional inter-firm relationships, which one would be more effective? Similarly, if one wished to invest in protecting a network to maintain its basic functionality, what are the potential tradeoffs with prolonging the total recovery time? Answers to these questions can be obtained by developing a more complete picture of SCNR and the relationship between its determinant factors.

Being thus motivated, we seek to answer the following research questions.

- What are the characteristics of a comprehensive and systematic measure of SCNR that can capture both the short-term and long-term impacts of a disruption?
- What are the determinants of supply chain network resilience and what are their relative effects on the different characteristics of SCNR?
- What are some of the potential tradeoffs between short-term and long-term resilience investments into SCNR?

The objective of this study is to provide a generalized, foundational approach for characterizing and assessing SCNR that future efforts can then easily adapt to a variety of other contexts. In this work, we thus perform a comprehensive and systematic investigation of SCNR in the presence of risk propagation. Specifically, we provide a quantitative framework to assess overall SCNR that considers both the short-term and long-term impacts of a disruption. As the whole SCN is composed of individual firms (nodes) and their supply relationships (links) (Borgatti and Li 2009), investments to improve SCNR can affect either the network structure (i.e., adding, deleting or rewiring links) (Zhao, Zuo, and Blackhurst 2019; Craighead et al. 2007) or individual firm risk capacity (i.e., strengthening nodes against a disruption) (Craighead et al. 2007); we therefore investigate how these factors influence the overall SCNR, and derive corresponding managerial implications.

The analyses below show that significant trade-offs exist between short-term and long-term resilience investments. They also show that actions which enhance node-level risk capacity are more effective than structural changes to the network for improving SCNR, and that network type has a larger influence on short-term impacts than it does on longer-term impacts. In addition, the results indicate that the choice of performance indicator by which resilience is assessed is critical for interpreting SCNR.

The remainder of the paper is organized as follows: Section 2 provides the literature review. Section 3 proposes the analytical network resilience framework and illustrates the calculation of SCNR. Section 4 conducts an in-depth analysis of how different impact factors influence SCNR, and Section 5 then provides some broader practical implications based on the analytical results. Finally, the discussion is summarized and conclusions are presented in Section 6.

2. Literature review

2.1 Supply Chain Network Resilience (SCNR)

The concept of supply chain resilience (SCR) originates from the supply chain risk management (SCRM) field (Christopher and Peck 2004; Ponomarov and Holcomb 2009). Traditional SCRM emphasizes managing risks along the supply chain and covers a wide range of topics, such as risk identification (Stephan M. Wagner and Bode 2006; Kleindorfer and Saad 2005), risk mitigation (Blackhurst et al. 2005; Tang 2006; Craighead et al. 2007), and supply chain recoverability (Kleindorfer and Saad 2005; Tomlin 2006). With supply chains becoming more complex and global in nature, the impact of regional disruptions can be far-reaching and long-lasting (Bode and Wagner 2015; Ivanov, Sokolov, and Dolgui 2014; Scheibe and Blackhurst 2017). Given that such disruptions are unavoidable and unpredictable in nature, supply chains must develop the capacity to adapt to their changing environment. This has led to considerable interest in supply chain resilience – the capability of the supply chain to prepare for, to respond to, and to recover from a disruption (Jüttner and Maklan 2011; Pettit, Croxton, and Fiksel 2013; Ponomarov and Holcomb 2009).

There has been a significant amount of academic interest in SCR. These studies mainly focus on outlining strategies for improving SCR, such as building logistics capabilities (Ponomarov and Holcomb 2009), investing in knowledge management (Jüttner and Maklan 2011; Sheffi and Rice Jr. 2005; Christopher and Peck 2004; Ponomarov and Holcomb 2009), strengthening supply chain integration and collaboration (Tang 2006; Pettit, Fiksel, and Croxton 2010; Christopher and Peck 2004; Świerczek 2014), increasing flexibility and visibility (Xia and Tang 2011; Pettit, Croxton, and Fiksel 2013; Tang 2006; Sheffi and Rice Jr. 2005), and improving network structure (Kim et al. 2011; Nair and Vidal 2011; Zhao et al. 2011; Craighead et al. 2007; Ivanov 2018a). It is common in the literature to refer to resilience as being associated not only with the response and recovery after a disruption, but also with resistance against that disruption (Li et al. 2019). Correspondingly, a number of studies measure SCR in the context of these two perspectives: robustness and recoverability (Bruneau et al. 2003). Robustness, also referred to as resistance (Dolgui, Ivanov, and Sokolov 2018) or absorptive capacity (Hosseini, Ivanov, and Dolgui 2019), is the supply chain's ability to withstand the impact from a disruption. Recoverability, also referred to as the capacity for recovery (Dolgui, Ivanov, and Sokolov 2018), is the supply chain's ability to restore functionality quickly after a disruption.

Because supply chains are complex networks consisting of interactive firms, and modern businesses no longer compete as solely autnomous entities but rather as whole supply chains (Lambert, Cooper, and Pagh 1998), there is a compelling need to study SCNR – the capacity of the entire supply network to respond to and recover from a disruption (Kim, Chen, and Linderman 2015; Zhao et al. 2011). Many studies focused on SCR are primarily conducted from a firm/node perspective that looks into the resilience capacity of a particular company or facility and only considers firm-level decision-making (Zobel and Khansa 2014; Zobel 2014; Pettit, Croxton, and Fiksel 2013; Pettit, Fiksel, and Croxton 2010). Extending this perspective to focus on the performance of the whole supply chain provides a more comprehensive view of the network's resilience behavior; this is particularly important for capturing the systemic risk that each firm is exposed to inside that network (Li et al. 2019). As an indication of the importance of this extended perspective, several recent studies specifically emphasize network level resilience (Zhao, Kumar, and Yen 2011; Zhao et al. 2011; Kim, Chen, and Linderman 2015; Nair and Vidal 2011), focusing on the whole supply chain’s performance after a disruption.

2.2 Risk propagation

It is important to recognize that many of the existing SCNR studies discussed above take a static approach to characterizing resilience, with relatively few of them considering the impact of risk propagation, or the ripple effect, in a complex network context (Basole and Bellamy 2014; Zhao, Zuo, and Blackhurst 2019). In practice, a disruption to a supply chain network often begins locally, with its impacts spreading to other firms through internal relationships. Consequently, the extent to which this occurs, and persists, could be considered to be a partial indicator of how resilient the network as a whole is to the disruption. Ignoring this ripple effect may result in misperceiving the nature of SCNR and underestimating the systemic risk faced by the supply chain. In recognition of the importance of this behavior, the literature contains a growing number of studies on supply chain risk propagation. These range from conceptual studies and literature reviews (Ivanov, Sokolov, and Dolgui 2014; Dolgui, Ivanov, and Sokolov 2018), to empirical studies that estimate risk propagation between interacting firms (Goto, Takayasu, and Takayasu 2017), qualitative studies that aim to understand what drives supply chain risk propagation (Scheibe and Blackhurst 2017), structural analyses of the interdependence of various risk drivers and supply chain performance (Srivastava, Chaudhuri, and Srivastava 2015; Chaudhuri et al. 2016), modeling efforts to characterize firms’ adaptive strategies against disruptions (Zhao, Zuo, and

Blackhurst 2019), and qualitative studies that investigate how network structure and supply chain visibility influence the level of risk propagation (Basole and Bellamy 2014).

Our research effort contributes, in particular, to the study of risk propagation from a complex network perspective (Basole and Bellamy 2014; Zhao, Zuo, and Blackhurst 2019; Li et al. 2019). Since modern supply chains are complex networks by nature, taking such a perspective helps to strengthen the applicability of the research results. In this context, risk propagation as a dynamic process results from the combined effect of the initial impact of the disruption, the network structure, and the firm-level risk capacities (Huang, Behara, and Hu 2008; Basole and Bellamy 2014). To understand the risk propagation process given the initial severity of a particular disruption, it is thus necessary also to consider how the network structure affects the resilience behavior of the supply chain.

2.3 Network Structure

SCN structure has been well recognized as a determining factor for SCNR (Kristianto et al. 2012; Snyder et al. 2012), and studies of the concept have been conducted from both a theoretical and a quantitative perspective. From the theoretical perspective, it is commonly considered that a supply chain is a complex network (Carter, Rogers, and Choi 2015), and it is suggested that the construction of a SCN consider not just the visible horizon boundary of the focal firm (Carter, Rogers, and Choi 2015) but also the scope of supply chain management (Lambert, Cooper, and Pagh 1998). In addition, the structure of a supply chain network may be defined in terms of the individual supply chain members and the process links (Lambert, Cooper, and Pagh 1998; Borgatti and Li 2009) or from an overall network perspective, and it can include consideration of such concepts as ego networks (Borgatti and Li 2009), triads (Choi and Wu 2009), and specific network properties (Kim et al. 2011; Borgatti and Li 2009; Choi and Krause 2006; Choi, Dooley, and Rungtusanatham 2001).

Quantitative studies that look at the ability of a supply network to resist and recover from disruptions mainly follow two types of approaches: traditional optimization approaches (Nagurney 2010) and network science approaches (Thadakamalla et al. 2004; Perera, Bell, and Bliemer 2017; Kim, Chen, and

Linderman 2015; Nair and Vidal 2011; Zhao et al. 2011). SCN structure has often been studied from a traditional optimization perspective, where researchers construct a network that satisfies all constraints and maximize supply chain performance using optimization methods (Snyder et al. 2012). Such an approach works well under the assumption of relatively small, static networks, but it is less effective for large-scale dynamic networks like those of most current global supply chains. Because of this limitation, the network science approach, which mainly focuses on comparing the relative performance of different network types, has emerged as an alternative (Wagner and Neshat 2010). Rather than looking at specific nodes and links, this approach investigates factors that can describe the network structure. The most frequently used such factor is the network type (Zhao et al. 2011; Kim, Chen, and Linderman 2015), which describes the interconnection patterns of the network. Such a focus has practical implications, since real SCN may often resemble a certain network type. For example, the electronics industry network is related to a small-world type of network, whereas the automotive industry is more similar to a scale-free type of network (Basole and Bellamy 2014).

Recent network science studies show, in particular, that network type has a significant impact on robustness - the ability to resist the impact of a disruption (Zhao et al. 2011; Thadakamalla et al. 2004; Nair and Vidal 2011; Kim, Chen, and Linderman 2015), and on the level of risk diffusion (Basole and Bellamy 2014). They also indicate that there may be trade-offs between these two aspects of network behavior. For example, although a scale-free network is especially robust against random disruptions (Nair and Vidal 2011; Zhao et al. 2011; Kim, Chen, and Linderman 2015), such a network may also accelerate risk diffusion (Basole and Bellamy 2014). This implies that a more comprehensive picture of SCNR over time is necessary in order to understand the true impact of particular factors.

3. SCNR framework

The complex nature of modern supply chain networks can make them challenging to study. For example, Ford has 1400 tier-one suppliers and up to 10 tiers of suppliers (Simchi-Levi et al. 2015), Nike's three-tier SCN contains 4036 nodes and 10949 edges, and General Mills' three-tier network has 1496 nodes and 4908 edges (Orenstein 2016). Responding to this complexity, this section defines a framework for measuring SCNR, in order to allow for exploring the resilience behavior of such networks.

3.1 SCN and disruption settings

We view the supply chain as a complex network in which nodes represent firms in the supply chain and links represent the interactive supply relationships between those firms (Carter, Rogers, and Choi 2015; Basole and Bellamy 2014; Zhao, Zuo, and Blackhurst 2019). From the perspective of modeling risk propagation, we view SCN as undirected because disruption risks can diffuse from both the supply side and the demand side (Ivanov 2017; Garvey, Carnovale, and Yeniyurt 2015; Ivanov 2018b). According to a recent survey (Gatepoint Research 2012), real-world supply chain disruptions originate almost equally between the demand side and tier-one suppliers. In this study, we consider a single random disruption that impacts one or more nodes in the network. This disruption can be caused by any type of risk, including a natural disaster, supplier failure, unplanned demand, or political and economic instability, and the severity of the disruption is measured by the number of nodes that it initially impacts. To isolate the effects of one disruption from another, we assume that there are no other major disruptions happening in a given observation period.

We use the concept of a disruption profile (Sheffi and Rice 2005) to characterize a SCN disruption. A typical disruption profile includes eight phases: preparation activities, the disruptive event, the first response, the initial impact, the full impact, the recovery preparations, and the recovery and long-term impact. Figure 1 shows a disruption profile with a disruption that occurs at time $t = 0$. It is generated by plotting a specific performance indicator, y_t, for each consecutive time period, $t \in \{0,1,\dots,T^*\}$. Here T is the time when the supply chain fully recovers from the disruption, t^{max} is the time when the system has the lowest performance after the disruption, and T^* is the time when a decision is made. To make different systems comparable, the performance is defined on a scale of zero to one, with a value of one representing full functionality.

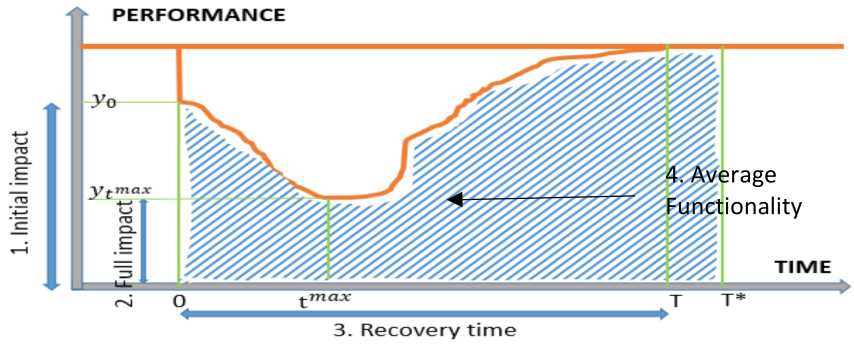


Figure 1: Disruption profile for a disruption that begins at time t=0

3.2 SCNR Measures

Given that SCNR represents the capability of the overall supply chain not only to maintain functionality after a disruption but also to quickly recover from that disruption, we adopt a subset of representative characteristics of the network performance indicators to measure this capability. This section presents a multi-dimensional resilience framework that is specifically based on the disruption profile.

3.2.1 SCNR dimensions

We focus, in particular, on three different dimensions of resilience behavior that may be derived from the disruption profile: the robustness, the recovery time, and the average functionality retained over time. These three measures, which are listed and defined in Table 1, are explained in detail below.

Robustness

Supply chain robustness measures the system's ability to absorb a disruption's impact and maintain functionality after that disruption occurs (Tierney and Bruneau 2007). According to this definition, a more robust system tends to perform better right after the disruption, and we would also expect higher robustness to lead to better performance at the time when the full impact of the disruption is realized. For this reason, we use both the performance at *initial impact* and at *full impact* to measure SCN robustness. In each case, a larger value of the measure represents a higher level of robustness.

$$Robustness_{initial-impact} = y_0 \qquad Robustness_{full-impact} = y_{t^{max}}$$

Recovery Time

System recoverability, or restorative capacity, connects with a system's capacity to restore full functionality in a timely manner (Tierney and Bruneau 2007). We use total *recovery time* to measure the system recoverability, where a longer recovery time represents a lower recoverability.

$Recovery\ Time = T$

Average functionality

Overall functionality captures the dynamic network performance over a period of time that typically starts with the outbreak of a disruption and ends after the system fully recovers (Ponomarov and Holcomb 2009; Tierney and Bruneau 2007; Sheffi and Rice 2005). This broader measure of the disruption's impacts not only effectively combines both robustness and recovery time, but also takes account of the speed at which the system recovers. Thus, we propose the third dimension of SCNR – average functionality, defined as overall average performance retained over time. This particular dimension is inspired by the concept of predicted resilience (Zobel 2011), and by related work that focuses on quantifying different types of resilient behavior (Zobel and Khansa 2012; Zobel 2014).

The average functionality is normalized by the total possible area so that it can be compared across networks of different sizes and complexities. As illustrated in Figure 1, it is thus defined as the area under the performance curve from time zero to time T^* (where T* represents the upper limit of the time frame of interest to the decision maker), divided by the length of that interval:

$$Average\ Functionality = \frac{1}{T^*}\int_0^{T^*} y_t dt$$

Here y_t represents the performance level at time *t*. In practice, supply chain performance is often recorded at distinct points in time, so we discretize the measure as in Table 1. The actual value of T* can be adjusted depending on the time frame over which the loss of performance is to be measured (Zobel 2014).

Table 1: Quantitative Network Resilience Framework

Dimension	Measure	Generalized Formula
Robustness	1. Robustness at initial impact	y_0
	2. Robustness at full impact	$y_{t^{max}}$
Recovery Time	3. Recovery time	T
Average Functionality	4. Average performance retained over time	$\frac{1}{T^*}\sum_{0}^{t=T^*} y_t$

3.2.2 Network performance indicators

The network performance, y_t, can be any quantitative measure that is related to overall SCN performance. Different network performance indicators that were used in previous studies are summarized in Table 2, along with their relationship to the components of our resilience framework. The *Largest Connected Component* (LCC) is the largest connected subnetwork at a certain time point after a disruption, the *average path length* (APL) is the average shortest path between any pair of nodes, and *Max. path length* (MPL) is the maximum shortest path among any pair of nodes. Each performance indicator describes a different aspect of supply chain performance. For example, total costs describe how a disruption influences operations (Nair and Vidal 2011), size of the LCC describes the network connectivity, APL and MPL describe network accessibility (Thadakamalla et al. 2004; Zhao et al. 2011), and the calculated measure from (Kim, Chen, and Linderman 2015) represents the likelihood of a network level disruption. Different performance indicators also have both pros and cons. Network-level financial indicators, such as sales, inventory level and costs, are easy to understand and apply, but generally require more assumptions. Structural measures, such as the size of the LCC and APL, are less intuitive to practitioners, but are easier to calculate and adapt to multi-product situations.

Table 2: Network performance indicators in existing quantitative studies.

Reference	Network Performance Indicator	Related Measures in the Resilience Framework	Static/ Dynamic
Nair & Vidal (2011)	Inventory level, Backorders Total costs	Robustness	Dynamic
Thadakamalla et al. (2004) Zhao et al., (2011)	Size of the LCC APL in the LCC MPL in the LCC	Robustness-Initial impact	Static
Kim et al., (2015)	$\frac{\text{Total number of node or arc disruptions that does not result a network disruption}}{\text{total number of node or arc disruptions}}$	Robustness-Initial impact	Static
Basole & Bellamy, (2014)	Change of healthy nodes	Robustness-Full impact	Dynamic

In order to illustrate the use of our quantitative resilience framework for SCNR, we select three specific network-level performance indicators to compare and contrast:

1. **Number of healthy nodes**. The total number of non-disrupted nodes can represent the overall health status of the network, and we divide it by the network size to normalize the impact of network size. Thus, the percentage of healthy nodes at time t can be calculated by $y_t = \frac{No.of\ healthy\ nodes\ at\ time\ t}{network\ size}$. This indicator has been used to measure the level of risk diffusion (Basole and Bellamy 2014).

2. **Size of the LCC**. Size of the LCC measures the number of healthy nodes in the LCC. When a disruption happens, the network may become disconnected and split into isolated subnetworks. The LCC is the largest fully-functioning subnetwork after a disruption, and a larger LCC indicates better network performance against the disruption (Thadakamalla et al. 2004; Zhao et al. 2011). Normalized by the network size, the corresponding performance indicator is $y_t = \frac{Size\ of\ the\ LCC\ at\ time\ t}{network\ size}$. The difference between the *number of healthy nodes* and the *size of the LCC* is the number of healthy nodes that are isolated from the LCC. Although these "external" nodes are isolated, once they are reconnected to the rest of the network recovery can be achieved quickly. In this sense, the two indicators provide different but complementary perspectives of network performance against disruptions.

Practically, the size of the LCC is a good indicator for systematic risks exposed to firms in the SCN. A smaller size of the LCC after a disruption implies that the whole supply chain suffers more and requires more efforts to recover from the disruption.

3. $\frac{\textbf{Size of the LCC}}{\textbf{APL of the LCC}}$. This ratio provides a network performance that incorporates supply chain efficiency. APL is generally used as an indication of supply chain efficiency in that a shorter APL indicates more efficient flow in the network (Albet, Jeong, and Barabasi 2000; Thadakamalla et al. 2004; Zhao et al. 2011). However, using only APL as a performance can be misleading as APL is highly correlated with the size of the LCC. For example, if one disruption makes the size of the LCC as small as two, the corresponding APL is one. Interpreting this small APL as representing high supply chain efficiency is misleading. Instead, we use the ratio $\frac{\text{Size of the LCC}}{\text{APL of the LCC}}$ as the third performance indicator because it not only is an effective measure of network performance that considers supply chain efficiency, but also it bypasses the misleading result of using APL. The performance indicator after normalization is then $y_t = \frac{Size\ of\ the\ LCC\ at\ time\ t/(APL\ of\ the\ LCC\ at\ time\ t)}{network\ size/(APL\ of\ the\ network)}$.

3.3 Modeling the risk propagation and recovery process

SCNR depends heavily on risk propagation and on the recovery behavior after a disruption. As a result, modeling the risk propagation and recovery process, especially before a disruption happens, is critical for estimating SCNR, and hence for supporting effective decision-making. The classic SIR model is one of the seminal frameworks used to understand risk propagation in epidemiology literature (Bailey 1977). This model consists of three states: S stands for susceptible, I for infectious, and R for recovered. In the supply chain field, Basole and Bellamy (2014) adapted this model to fit an MTG model, with three states: Good, Moderate and Toxic, in order to investigate the relationship between network structure, supply visibility and levels of risk propagation. Similarly, we also adapt the SIR model to fit the risk propagation and recovery process.

In our work, we assume that a node has three states: healthy (susceptible), healthy (immune), and disrupted. A healthy node can be either susceptible to infection or immune. A healthy (susceptible) node can become disrupted in the next period if any of its neighbors is in a disrupted status. Once a disrupted node is recovered, it gains immunity and achieves healthy (immune) status, in which it will not be influenced by the original disruption risk anymore. Figure 2 illustrates the process of transition between node states. The infection probability, $p_{infection}$, is the probability that a healthy (susceptible) node will become disrupted in the next time period due to its infectious neighbors. Similarly, the recovery probability, $p_{recovery}$, is the probability that a disrupted node recovers in the next time period.

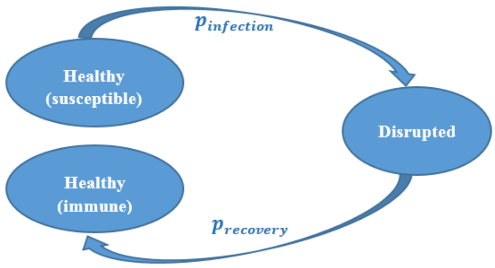


Figure 2: Node status transition

We summarize assumptions below that were made in order to have an appropriately descriptive and necessarly complex model of the risk propagation process:

- There is a single disruptive event

We assume that the network is only suffering from the cascading effects of a single disruption, and that there are no other types of disruptions introduced during the risk propagation and recovery process.

- Disruption happens at the node-level.

We only consider node-level disruptions because we view the links in the network as the relationships between firms, rather than as the physical route from one to another. From the viewpoint of material ownership, the loss from a disruption is either suffered by the supplier side or by the customer side. In practice, even if a disruption happens during transportation between firms, the material ownership is either of the supplier or of the customer, thus it is essentially equivalent to a node-level disruption.

- The state of each node is known with certainty.

For the purposes of characterizing the effects of risk propagation across the entire supply chain network, we assume that the current state of each node, as defined above, is known at any given point in time.

- Firms gain "immunity" after recovery.

We assume a firm can gain sufficient experience and capability to avoid being infected again by the same disruptive event after the firm recovers. This is supported by a number of real-world cases. For example, Toyota and its suppliers ordered substitute auto parts from China and even contracted with competitors to produce parts on their behalf until their operations resumed during the 2011 Tohoku earthquake and tsunami (Greimel 2016). These adopted approaches protected Toyota and its suppliers from being re-infected again by the supply shortage after the earthquake.

- Homogeneous node risk capacity across the network.

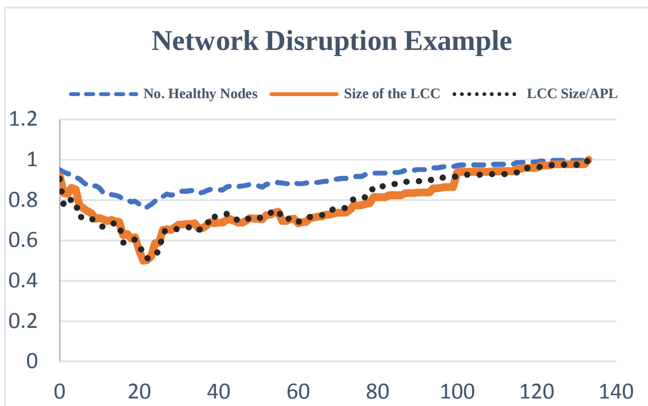
Node risk capacity is the capability of a node to resist and then quickly recover from a disruption. This is effectively the individual node resilience. Both $p_{infection}$ and $p_{recovery}$ therefore represent aspects of the node risk capacity. For the sake of simplicity, in this particular paper we assume that $p_{recovery}$ and $p_{infection}$ are the same for all nodes across the network. Although this may not completely capture the complexity of the real-world, it gives us a good basis for understanding how node risk capacity influences overall SCNR.

3.4 Illustrative example and determining factors of SCNR

In this section, we illustrate how to calculate SCNR, using the Japanese auto supply network as the data source and the NetLogo 5.3 modeling platform (Wilensky 1999) as the simulation tool. NetLogo is a justified powerful agent-based simulation platform, which is well designed and documented, and easy to learn and use (Lytinen and Railsback 2012). The network data were extracted from the Bloomberg SPLC database, based on the theory that the supply chain is a complex network that exists relative to a particular product/agent and is bounded by the visible horizon of the focal agents (Carter, Rogers, and Choi 2015). We select Honda and Toyota as the focal firms because these two are the largest automobile makers in Japan. Then we construct a set of first and second tier suppliers of these two focal firms, in which a supplier is included only if its percentage of COGS (Cost Of Goods Sold) is over 1%. This gives us a network with 302 nodes and 404 links.

Next, we simulate a 5% disruption severity by randomly disrupting 15 nodes. Assuming that all nodes have a recovery probability of 5% and an infection probability of 10%, we record the three selected performance indicators at each time period and calculate the resulted network robustness, recovery time, and average functionality according to Table 1. Under the settings above, a single run of this simulated disruption takes 133 steps to reach total recovery of the network. To reflect both the short-term and long-term performance, we use $T^* = 50$ and $T^* = 150$ to calculate the average functionality over each of those time periods. Table 3 shows the network, the simulated risk propagation and recovery process, and the calculated SCNR measures from a single run of the simulation. Several patterns emerge from this: First, the characteristic shape of each performance indicator's profile echoes the theoretical disruption profile model in Figure 1; Second, although the recovery time is the same for each network performance indicator, the different dimensions of SCNR vary across the network performance indicators.

Table 3: Calculation illustration

	
Japanese Auto SCN No. nodes: 302 No. links: 404	Disruption Severity: 5% (15 nodes) Recovery probability: 5% Infection probability: 10%

	Robustness		Recovery Time (steps)	Average Functionality	
	Initial Impact	Full Impact		$T^* = 50$	$T^* = 150$
No. Healthy nodes	0.950	0.761	133	0.865	0.925
Size of the LCC	0.921	0.500	133	0.701	0.818
$\frac{\text{Size of the LCC}}{\text{APL of the LCC}}$	0.905	0.507	133	0.690	0.822

SCNR depends not only on disruption severity but also on network structure and node risk capacity. Network structure, which influences the direction and level of risk propagation, can be described by both network type and network complexity. Node risk capacity, or node resilience, which is a firm's ability to maintain functionality in a disturbed environment, also has an impact on the risk propagation and recovery process (Huang, Behara, and Hu 2008; Brusset and Teller 2017). This capacity can be measured by the combination of risk infection probability and recovery probability, where a firm with lower risk infection probability and higher recovery probability will tend to have a higher risk capacity. Figure 3 thus depicts the relationship between disruption severity, network structure, node risk capacity, and SCNR.

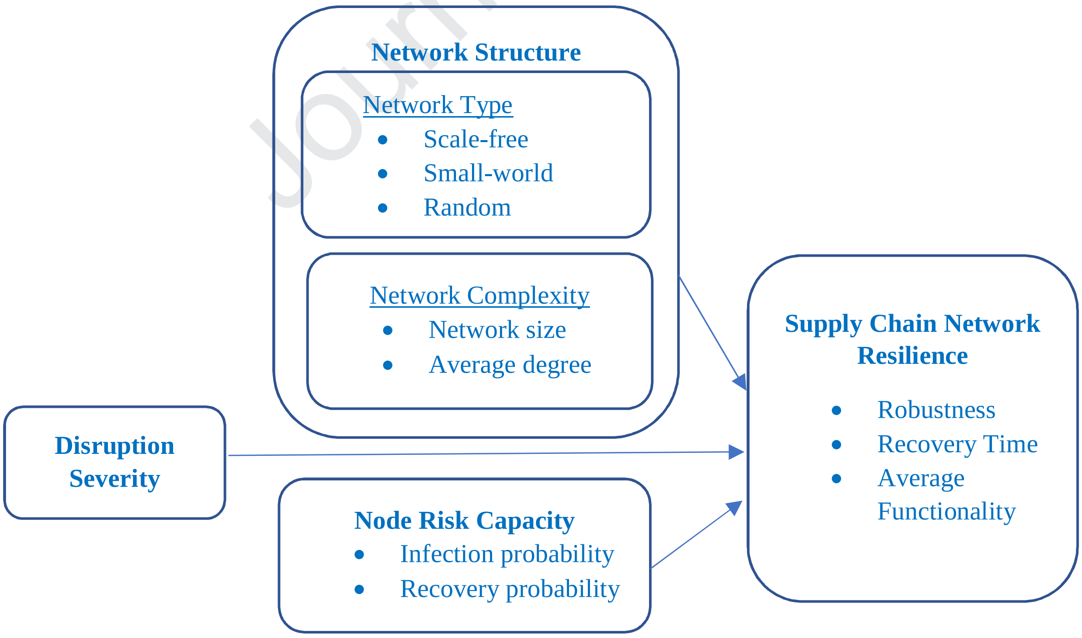


Figure 3: Determining factors of network resilience

4. Network resilience analysis

Our proposed framework uses simulation and regression analysis to systematically explore the impacts of network structure and node risk capacity on SCNR. Simulation is widely used in business modeling when it is impossible or impractical to conduct experiments on a real system, and a number of previous research efforts related to supply chain disruptions (Nair and Vidal 2011; Macdonald et al. 2018; Melnyk et al. 2014) and to risk propagation (Basole and Bellamy 2014; Hua, Sun, and Xu 2011) have used regression as a tool for analyzing simulated data. Regression is generally applicable for analyzing high-dimensional data where the underlying model is uncertain (Hanaki et al. 2007; Basole and Bellamy 2014), and the approach is flexible enough to include both continuous and categorical variables. Furthermore, previous studies have also utilized regression to investigate the impact of network structure on network health status (Basole and Bellamy 2014). The design of our experiment is motivated by previous studies on SCN and on the characteristics of real-world SCNs. The full factorial design considers all possible combinations of parameter levels across each of the independent variables and controls, and it results in a total of 2304 distinct observations. A summary of the experimental design is presented in Table 4, and the parameter settings for each variable are explained in more detail below.

Table 4: Experimental Design.

Variables	**Notation**	**Levels**
Control Variables		
Disruption Severity	Dis_sev	(10%, 30%, 50%, 70%)
Independent Variables		
Network Types	Net_type	(Scale-free, Small-world, Random)
Network Size	Net_size	(100, 300, 500)
Average Degree	Ave_degree	(2,4,6,8)
Recovery Probability	Rec_pro	(20%, 40%, 60%, 80%)
Infection Probability	Inf_pro	(20%, 40%, 60%, 80%)
Total observations: $3 * 3 * 4 * 4 * 4 * 4 = 2304$		

4.1 Experimental design

4.1.1 Control variables

Disruption severity, defined as the percentage of nodes directly impacted by the disruption, has a significant impact on SCNR. Because the severity of a disruption is typically beyond the control of policymakers, however, we choose it as a control variable in our experiment. We set the disruption severity levels to vary from 10% to 70%, to provide a wide range of representative disruptions.

4.1.2 Independent variables

The independent variables are associated with network structure and node risk capacity. We use three variables to describe network structure: network type, network size and average degree. Network type is widely used to represent the general pattern of connections among nodes within a network, while network size and average degree together measure the network complexity. The variables used to measure node risk capacity are node infection probability and recovery probability.

Network Type

We focus on three types of network in this study: scale-free, small-world, and random. These are the most frequently studied SCN types (Thadakamalla et al. 2004; Zhao et al. 2011; Kim, Chen, and Linderman 2015; Nair and Vidal 2011) because many real-world supply chains resemble the characteristics of scale-free and small-world networks (Basole and Bellamy 2014; Perera, Bell, and Bliemer 2017). A random network, which is a type of network in which every pair of nodes has the same likelihood of being connected, is generally used as a benchmark for comparatively assessing the performance of the other network types (Nair and Vidal 2011; Basole and Bellamy 2014), as we do here. Below are the characteristics of each network type in detail.

The scale-free network, which characteristically has an exponential degree distribution, is the most widely studied network type in the supply chain field (Zhao et al. 2011; Basole and Bellamy 2014; Nair and Vidal 2011; Kim, Chen, and Linderman 2015). A scale-free network generally contains a few nodes with many links, called hubs, and a large number of nodes with few links. This characteristic makes the scale-free network robust to random disruptions because this robustness is based on the average performance and a disruption has a low probability of directly impacting the few hub-nodes. Many real networks belong to the scale-free type, including the automobile industry (Basole and Bellamy 2014), pork supply chain (Büttner et al. 2013), Airbus supply chain (Brintrup, Wang, and Tiwari 2015), food and retail supply chain (Orenstein 2016) and the Wal-Mart distribution system (Holmes 2011).

The small-world network has the characteristic that most interactions are local, and few links exist between any given node and another distant node. The clustering coefficient of a small-world network is close to that of regular lattice network, which is much higher than that of a random network, and a small-world network has been shown to have an APL similar to that of a random network (Watts and Strogatz 1998). Real-world examples of small-world networks include the ownership of German firms, academic collaboration networks, firm alliance networks, and electronic industry supply networks (Rivkin and Siggelkow 2007; Basole and Bellamy 2014; Kim, Chen, and Linderman 2015).

Network Complexity

Network complexity, in turn, can be measured by network size and average degree (Craighead et al. 2007; Choi and Krause 2006). Network size is the number of nodes in the network, and the average degree has a linear relationship with the total number of links for a given network: $\boldsymbol{Average\ degree} = \frac{\mathbf{2} * \boldsymbol{Num\_links}}{\boldsymbol{Num\_nodes}}$. The average degree of a network represents both the connectedness and clustering of that network. A higher value for average degree represents more links in a network, and hence more complexity.

Our parameter settings for network size and average degree are motivated by recent studies, since SCN size can vary significantly depending on the nature and scope of the analysis. Specifically, Zhao et al. (2011) examine SCNR using a network size of 1000 with an average degree of 3.6, and Basole and Bellamy (2014) look at network sizes ranging from 100 to 1000, with an average degree ranging from 2 to 20. Based on these studies, we chose to vary our network size from 100 to 500, with an average degree range of 2 to 8. These represent moderately sized SCNs.

Understanding the association between network complexity and SCNR can be very important for supply chain managers. In practice, supply chain managers can increase or decrease the number of links in their network to achieve better performance.

Node Risk Capacity

We use the combination of infection probability and recovery probability to measure node risk capacity. For both parameters, we chose values ranging from 20% to 80% in order to represent a wide range of risk propagation behaviors. Practitioners can potentially improve these rates by investing in resources such as extra stock, backup suppliers, IT functionality, or emergency planning. Therefore, gaining more insights into the relationship between risk propagation and network resilience can support more informed decision-making on related investments.

4.1.3 Dependent variables and models

The dependent variables in the analysis are the different components of SCNR: robustness at initial impact ($Robust\_II$), robustness at full impact ($Robust\_FI$), recovery time (RT), and average functionality (AF), each one calculated based on three network performance indicators: the number of healthy nodes, the size of LCC, and $\frac{\textbf{Size of the LCC}}{\textbf{APL of the LCC}}$. To investigate the relationship between independent variables and these dependent variables, we use the seemingly unrelated regression (SUR) model, as it is able to evaluate relationship between a set of correlated dependent variables and different sets of exogenous explanatory variables. Below are the detailed model specifications.

$$\begin{cases} Robust\_II_i = \beta_{10} + \beta_{11}Dis\_sev_i + \beta_{12}Net\_type_i + \beta_{13}Net\_size_i + \beta_{14}Ave\_degree_i + \beta_{15}Rec\_pro_i + \beta_{16}Inf\_pro_i + \varepsilon_{1i} \\ Robust\_FI_i = \beta_{20} + \beta_{21}Dis\_sev_i + \beta_{22}Net\_type_i + \beta_{23}Net\_size_i + \beta_{24}Ave\_degree_i + \beta_{25}Rec\_pro_i + \beta_{26}Inf\_pro_i + \varepsilon_{2i} \\ RT_i = \beta_{30} + \beta_{31}Dis\_sev_i + \beta_{32}Net\_type_i + \beta_{33}Net\_size_i + \beta_{34}Ave\_degree_i + \beta_{35}Rec\_pro_i + \beta_{36}Inf\_pro_i + \varepsilon_{3i} \\ AF_i = \beta_{40} + \beta_{41}Dis\_sev_i + \beta_{42}Net\_type_i + \beta_{43}Net\_size_i + \beta_{44}Ave\_degree_i + \beta_{45}Rec\_pro_i + \beta_{46}Inf\_pro_i + \varepsilon_{4i} \end{cases}$$

The subscript *i* stands for each observation.

4.2 Results and analyses

To generate the data for our analysis, we simulate each scenario in Table 4. We replicate each scenario 30 times to average out the stochastic effects. The total period chosen for the calculation of AF

retained is T*=50, which is longer than the maximum recovery time of any of the replications. Table 5 shows the descriptive statistics of the variables.

We run our analyses in STATA 14.1 and present the SUR regression results for the different network performance indicators in Tables 6-8, from which we summarize Table 9. As expected, given the nature of the experiment design, these independent variables are independent based on our data. We also conducted a robustness check using a simultaneous equations model and the results are consistent with those of the SUR model.

Table 5: Descriptive Statistics

	N	Mean	Standard Deviation	Min	Max
Independent Variables					
Dis_sev	2304	40	22.36553	10	70
Net_size	2304	300	163.3348	100	500
Ave_degree	2304	5	2.236553	2	8
Rec_prob	2304	50	22.36553	20	80
Inf_prob	2304	50	22.36553	20	80
Dependent Variables					
Number of Healthy Nodes as Network Performance Indicator					
$Robust\_II$	2304	.6	.2236553	.3	.9
$Robust\_FI$	2304	.5316207	.211473	.1903333	.9
RT	2304	13.37079	9.467874	2.366667	42.33333
AF	2304	.9633217	.0290435	.9026133	.9974133
Size of the LCC as Network Performance Indicator					
$Robust\_II$	2304	.4737241	.2944265	.0123303	.9
$Robust\_FI$	2304	.3810829	.2675571	.0106	.9
RT	2304	13.37079	9.467874	2.366667	42.33333
AF	2304	.9459654	.050766	.6951378	.9970593
$\frac{Size\ of\ the\ LCC}{APL\ of\ the\ LCC}$ as Network Performance Indicator					
$Robust\_II$	2304	.4535413	.269155	.0453899	.8886256
$Robust\_FI$	2304	.3543417	.2351857	.0314077	.8838721
RT	2304	13.37079	9.467874	2.366667	42.33333
AF	2304	.9439041	.0449719	.7888132	.9961957

4.2.1 Direct impact of network structure

Network Type

Our results show that network type influences varied aspects of SCNR differently. In general, the impact of network type on SCNR is mainly in the short-term ($\boldsymbol{Robust\_II}$), and less in the long-term (the $\boldsymbol{Robust\_FI}$ and $\boldsymbol{RI}$). Moreover, this impact relies on the selection of the network performance indicator.

For a scale-free network, our results echo the previous finding that such a network is particularly robust at initial impact in terms of measuring the size of the LCC and the APL (Thadakamalla et al. 2004; Albet, Jeong, and Barabasi 2000; Zhao et al. 2011) for a random disruption. Our results also show that it has no significant impact on SCNR when the performance indicator is the number of healthy nodes, and it has no significant impact on $\boldsymbol{Robust\_FI}$ and $\boldsymbol{RT}$. This is because, under the assumption of node immunity, the network can gain robustness after the hub nodes have immunity, which hampers the risk diffusion afterward and offsets the initial negative impact. Considering that a scale-free network can accelerate risk propagation and result in less favorable network health when nodes don't gain immunity after a disruption (Basole and Bellamy 2014), it is important to focus attention on preventing the hub nodes from getting re-infected in practice.

For the small-world network, our results are consistent with a previous study that shows a small-world network tends to have a smaller size of LCC after a disruption, compared to a random network (Thadakamalla et al. 2004). Also, for performance indicator $\frac{\textbf{\textit{Size of the LCC}}}{\textbf{\textit{APL of the LCC}}}$, the small-world network is robust because of the increased level of "small-worldness" after the disruption (Jalili 2011). Small-worldness is a measure of the degree of the small-world pattern by comparing the APL and clustering coefficient of a random network. This increasing small-worldness means that a small-world network tends to have a smaller APL and a bigger clustering coefficient when more nodes are removed. Similar to the scale-free network, the small-world network also does not have a significant impact on recovery time.

Table 6: Number of Healthy Nodes as Network Performance Indicator

	$Robust\_II$ b/se	$Robust\_FI$ b/se	RT b/se	AF b/se
Controls				
Dis_sev	-0.0100	-0.0080***	-0.0175***	-0.0003***
	(.)	(0.000)	(0.003)	(0.000)
Direct effect				
Scale_free		0.0010	-0.0973	0.0002
		(0.004)	(0.177)	(0.001)
Small_world		-0.0011	0.0601	-0.0002
		(0.004)	(0.177)	(0.001)
Net_size		0.0000	0.0087***	0.0000
		(0.000)	(0.000)	(0.000)
Ave_degree		-0.0133***	0.0784*	-0.0012***
		(0.001)	(0.032)	(0.000)
Rec_prob		0.0032***	-0.3881***	0.0011***
		(0.000)	(0.003)	(0.000)
Inf_prob		-0.0012***	-0.0074*	-0.0001***
		(0.000)	(0.003)	(0.000)
Constant		0.8133***	30.8560***	0.9280***
		(0.008)	(0.359)	(0.001)
Number of observations	2304	2304	2304	2304
R-squared	1.00	0.87	0.87	0.84
p-value	0.00	0.00	0.00	0.00
p-value for Breusch-Pagan test of independence		0.0000		

Standard errors in parentheses * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Network Complexity

Our results show that network complexity (network size and average degree) significantly influences every aspect of SCNR. Network size has a negative but negligible impact on SCNR, with an increase in network size leading to a decrease in robustness, longer recovery time, and lower average functionality. However, an increase of 100 nodes in network size can only decrease 0.0001 of the size of the LCC right after the disruption and it only increases the recovery time by 0.87 steps. In practice, such an influence is too small to be operative. This practical insignificance is also seen with respect to the other measures of SCNR, which is consistent with the previous finding that network robustness is independent of the network size (Albet, Jeong, and Barabasi 2000) in the parameter space. This finding allows us to compare the performance of SCNs of different sizes on the same basis.

Table 7: Size of the LCC as Network Performance Indicator

	Robust_II b/se	*Robust_FI* b/se	*RT* b/se	*AF* b/se
Controls				
Dis_sev	-0.0110***	-0.0084***	-0.0175***	-0.0004***
	(0.000)	(0.000)	(0.003)	(0.000)
Direct effect				
Scale_free	0.0136**	0.0006	-0.0973	0.0028
	(0.005)	(0.006)	(0.177)	(0.001)
Small_world	-0.0183***	-0.0073	0.0601	-0.0050***
	(0.005)	(0.006)	(0.177)	(0.001)
Net_size	-0.0001***	-0.0000*	0.0087***	-0.0000***
	(0.000)	(0.000)	(0.000)	(0.000)
Ave_degree	0.0566***	0.0485***	0.0784*	0.0079***
	(0.001)	(0.001)	(0.032)	(0.000)
Rec_prob	-0.0000	0.0041***	-0.3881***	0.0017***
	(0.000)	(0.000)	(0.003)	(0.000)
Inf_prob	-0.0000	-0.0014***	-0.0074*	-0.0001***
	(0.000)	(0.000)	(0.003)	(0.000)
Constant	0.6500***	0.3512***	30.8560***	0.8457***
	(0.010)	(0.013)	(0.359)	(0.003)
Number of observations	2304	2304	2304	2304
R-squared	0.89	0.79	0.87	0.70
p-value	0.00	0.00	0.00	0.00
p-value for Breusch-Pagan test of independence		0.0000		

Standard errors in parentheses * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 8: $\frac{\boldsymbol{Size\ of\ the\ LCC}}{\boldsymbol{APL\ of\ the\ LCC}}$ as Network Performance Indicator

	$Robust\_II$ b/se	$Robust\_FI$ b/se	RT b/se	AF b/se
Controls				
Dis_sev	-0.0114***	-0.0081***	-0.0175***	-0.0003***
	(0.000)	(0.000)	(0.003)	(0.000)
Direct effect				
Scale_free	0.0244***	0.0057	-0.0973	0.0037***
	(0.003)	(0.005)	(0.177)	(0.001)
Small_world	0.0086**	0.0213***	0.0601	0.0002
	(0.003)	(0.005)	(0.177)	(0.001)
Net_size	-0.0001***	-0.0001***	0.0087***	-0.0000***
	(0.000)	(0.000)	(0.000)	(0.000)
Ave_degree	0.0271***	0.0170***	0.0784*	0.0040***
	(0.001)	(0.001)	(0.032)	(0.000)
Rec_prob	0.0000	0.0042***	-0.3881***	0.0017***
	(0.000)	(0.000)	(0.003)	(0.000)
Inf_prob	-0.0000	-0.0013***	-0.0074*	-0.0001***
	(0.000)	(0.000)	(0.003)	(0.000)
Constant	0.7992***	0.4787***	30.8560***	0.8586***
	(0.006)	(0.011)	(0.359)	(0.002)
Number of observations	2304	2304	2304	2304
R-squared	0.95	0.81	0.87	0.82
p-value	0.00	0.00	0.00	0.00
p-value for Breusch-Pagan test of independence		0.0000		

Standard errors in parentheses * p < 0.05, ** p < 0.01, *** p < 0.001

In contrast, the impact of average degree on different aspects of SCNR varies across the different performance indicators. When the performance indicator is the number of healthy nodes, average degree negatively influences SCNR, with a larger average degree leading to lower $\boldsymbol{Robust\_FI}$, higher $\boldsymbol{RT}$, and lower $\boldsymbol{AF}$. When the performance indicator is the size of the LCC, or $\frac{\boldsymbol{Size\ of\ the\ LCC}}{\boldsymbol{APL\ of\ the\ LCC}}$, however, it is positively correlated with all four resilience measures. These results imply that we should be aware of the trade-offs among different aspects of resilience. For example, when investing in network connectivity, practitioners should consider all the possible benefits and costs, and evaluate the overall impact on SCNR.

Table 9: Direct impact of independent variables.

				Robustness		RT	AF
				$Robust\_II$	$Robust\_FI$		
Network Structure	Network Type	Scale-free	No. healthy nodes		No	No	No
			Size of the LCC	+	No	No	No
			Size of the LCC / APL of the LCC	+	No	No	+
		Small-world	No. healthy nodes		No	No	No
			Size of the LCC	-	No	No	-
			Size of the LCC / APL of the LCC	+	+	No	No
	Network Complexity	Network Size	No. healthy nodes		No	+	No
			Size of the LCC	-	-	+	-
			Size of the LCC / APL of the LCC	-	-	+	-
		Average degree	No. healthy nodes		-	+	-
			Size of the LCC	+	+	+	+
			Size of the LCC / APL of the LCC	+	+	+	+
Node Risk Capacity		Recovery Probability	No. healthy nodes		+	-	+
			Size of the LCC	No	+	-	+
			Size of the LCC / APL of the LCC	No	+	-	+
		Infection Probability	No. healthy nodes		-	-	-
			Size of the LCC	No	-	-	-
			Size of the LCC / APL of the LCC	No	-	-	-

+ means there is a significant positive relationship; - means there is a significant negative relationship; No means there is no significant relationship; The shaded grid means the situation is not suitable for the associated calculation. This is because the initial impact is the same as the disruption severity in terms of the number of healthy nodes.

4.2.2 Direct impact of the node risk capacity

Both indicators of node risk capacity: recovery probability and infection probability, have significant impacts on $\boldsymbol{Robust\_FI}$, on $\boldsymbol{RT}$, and on $\boldsymbol{AF}$. Since recovery probability and infection probability mainly work during risk propagation process, they do not have an impact on the $\boldsymbol{Robust\_II}$. Our results show that node recovery probability is positively associated with SCNR: higher node recovery probability can increase $\boldsymbol{Robust\_FI}$ and $\boldsymbol{AF}$, and it can decrease the $\boldsymbol{RT}$. Because node recovery probability represents an individual node's capability to recover from a disruption, in practice a company can increase its recovery probability by having backup suppliers and by implementing efficient risk mitigation methods. These activities can both decrease loss and lower total recovery time.

Infection probability, however, is negatively associated with $\boldsymbol{Robust\_FI}$, $\boldsymbol{RT}$, and $\boldsymbol{AF}$. A lower infection probability represents less likelihood that a given firm can be influenced when exposed to risks. A company can decrease its infection probability by adopting a multi-supplier procurement strategy or increasing its stock level to enhance the capability to protect against a disruption. Increasing the infection probability, on the other hand, will accelerate the risk propagation and lead to lower robustness. We also observe that a higher infection probability is associated with a shorter $\boldsymbol{RT}$. This is because even though a higher infection rate will cause lower robustness in the short-term, the immunity of the recovered nodes will lead a quick recovery time for the whole system. Taking the extreme case as an example, if the infection probability is one then all nodes will be disrupted within a few steps. Once these nodes recover, they gain immunity and will not get disrupted again. As the total recovery time is the time when last node recovers, in this situation, total recovery time is normally shorter than that of a process that experiences a longer risk propagation period and then recovers.

5. Implications

From the above analyses, we summarize several important implications.

1. The influence of network type on SCNR is mainly associated with short-term effects, and less so with long-term effects.

Network type represents the interacting relationship among nodes in a network given the network size and average degree. Our results show that when the performance indicator is the number of healthy nodes, then network type does not have an impact on SCNR. When the chosen performance indicator is size of the LCC and $\frac{\text{Size of the LCC}}{\text{APL of the LCC}}$, network type influences $Robust\_II$ (short-term effect), but not the longer-term resilience measures, such as $Robust\_FI$, RT, and AF. This means that in the presence of risk propagation, the connection pattern represented by the different network types has less effect on the network performance later on. However, we also observe an exception, in that the small-world network has a negative effect on average functionality when measuring the size of the LCC, and it has a positive effect on $Robust\_FI$ when measuring $\frac{\text{Size of the LCC}}{\text{APL of the LCC}}$. This implies that network types may be too general of a means for representing the network connection pattern to truly explain the effect on SCNR.

Besides network type and network complexity, a combination of network characteristics can also describe a network. A network characteristic describes one particular facet of the network structure. For example, the clustering coefficient measures the degree to which nodes in a network tend to cluster together, and the APL depicts the average of the shortest path length between any pair of nodes. In addition, because not all networks can be classified as a particular network type, but any given type of network can always be described by a combination of network characteristics, network characteristics can provide a more precise means of capturing network behavior. Considering that the current literature on SCN mainly focuses on network types (Kim, Chen, and Linderman 2015; Zhao et al. 2011; Basole and Bellamy 2014; Nair and Vidal 2011), we propose that focusing on network characteristics can thus lead to a better understanding of how network structure influences SCNR.

2. Compared with adjusting network structure, enhancing node risk capacity is more effective for improving SCNR, especially with the existence of risk propagation.

We use network type, network size and average degree to describe the network structure. In our analysis, the impact of network type on SCNR is mainly observed in the short-term, and very limited in the long-term, while the impact of network size is practically negligible. Also, it is costly to increase average degree substantially because increasing average degree by two represents increasing the total number of links by the network size. For example, for a network with 100 nodes, increasing average degree by two represents adding additional 100 links. Such a substantial increase can cause higher operational cost for communication and collaboration. Moreover, although increasing average degree can lead to higher robustness, it also causes longer total recovery time. Comparatively, enhancing node risk capacity is more effective, especially because increasing recovery probability can both increase robustness and decrease the total recovery time. In practice, activities used to increase recovery probability include increasing visibility within the supply chain, adopting a higher level of stock, and contracting with backup suppliers.

Given the importance of node risk capacity to SCNR and the impracticality of enhancing the risk capacity of every node inside the network, selecting critical nodes in which to invest to maximize SCNR is necessary for both researchers and practitioners. Considering that current studies of critical nodes' effects on disruptions are mainly conceptual (Craighead et al. 2007; Ponomarov and Holcomb 2009) and focus on short-term disruption impacts, we, therefore, propose looking at critical nodes that can build SCNR both short-term and long-term.

3. Trade-offs exist between robustness and recovery time.

An ideal investment in SCNR would increase robustness and decrease total recovery time simultaneously. However, increasing robustness may lead to longer recovery time in some cases. From our results, when the performance indicator is the size of the LCC, increasing average degree results in both higher robustness and longer recovery time. Similarly, decreasing the infection probability results in higher robustness but longer recovery time. Because this trade-off between robustness and recovery time is the trade-off between short-term and long-term benefits, in practice, practitioners should evaluate the overall effect of their mitigation and recovery decisions in order to achieve more effective overall results. This also implies that for future research on SCNR, evaluating a certain strategy should consider both the short-term and long-term effects, so as to build a more comprehensive understanding of SCNR.

4. Selecting network performance indicators is critical for interpreting SCNR.

Our study selects three different network performance indicators for the purposes of demonstration, each providing a different perspective. Our analyses indicate that the resilience behaviors of these different performance indicators vary. For example, increasing the average degree will decrease $Robust\_FI$ when measuring the number of healthy nodes, but it will increase that robustness for the other two network performance indicators. It is thus important to clearly specify which aspects of the network are exhibiting which types of resilient behavior, as different performance indicators may lead to varying outcomes. Practitioners should evaluate not only the behavior of a preferred performance indicator, but also the corresponding behaviors of other informative performance indicators. A SCN may be resilient in different ways under different circumstances, and investments into improving resilience should be based on a comprehensive understanding of resilience behavior across various performance indicators.

As mentioned above, our simulation model is adapted from the SIR model, which only considers the number of healthy nodes after the disruption. We expanded this to look at the size of the LCC and $\frac{\text{Size of the LCC}}{\text{APL of the LCC}}$ as alternative performance indicators. While the number of healthy nodes represents the overall health status of the network, the size of the LCC instead describes the network connectivity, and $\frac{\text{Size of the LCC}}{\text{APL of the LCC}}$ depicts both the network connectivity and network efficiency. As resilience behaviors vary for different performance indicators, our work contributes to the network risk propagation literature by illustrating the potential for measuring resilient behavior more holistically.

5. This resilience framework can be extended based on practical needs.

The proposed framework provides support for a systematic and comprehensive understanding of SCNR. This framework can be extended in a number of different ways, in practice, to support effective decision-making. First of all, additional resilience dimensions could be added depending on the type of decisions that will be made. For example, $\mathrm{T}^{\max}$, the length of time between when the disruption happens and the full impact is realized (see Figure 1), can provide additional information about how quickly the system can start to recover. A practitioner may want to invest in deriving better information about $\mathrm{T}^{\max}$ in order to prepare more effectively for recovery. Different values of T* could also be used to calculate short-term average functionality retained, mid-term average functionality retained, or long-term average functionality retained. The framework could also be expanded by adding additional network performance indicators, such as average path length (APL) and maximum path length (MPL). Furthermore, if the generalized model presented above were adapted to incorporate specific behaviors such as directional material flows, it could be used to analyze more detailed supply chain measures such as total sales and total customer satisfaction. The framework thus contributes to the literature of SCNR by providing a generalized, fundamental approach for assessing SCNR that future efforts can easily build upon to explore other aspects of SCNR.

6. Conclusion

This paper explores SCNR in the presence of risk propagation, and in doing so it makes several important theoretical and practical contributions to the literature. Theoretically, this study enriches the literature of SCNR by focusing on risk propagation and proposing a multi-dimensional resilience metric to quantify both short-term and long-term resilience behaviors. It also contributes to the literature by conducting a systematic analysis of the determining factors of SCNR: network structure and node risk capacity, and their effects on risk propagation and the different characteristics of resilient behavior.

This study also provides a number of practical implications for decision-makers, to help them better understand SCNR in terms of the systemic risk faced by individual firms inside the network. As illustrated in Section 3.4, practitioners can estimate SCNR for a given network using different settings for disruption severity and node risk capacity. This allows them to assess the short-term and long-term behavior of a network after a disruption, and it can help them to formulate proper sourcing, production, and marketing strategies to prepare for potential disruptions and to gain a competitive advantage in a risky environment. Moreover, our findings can potentially support decision makers in making proactive investments to improve SCNR. Our results clearly present how network structure and node risk capacity influence different aspects of SCNR. By considering related practical activities that are associated with these factors, practitioners could compare different operational strategies for improving SCNR.

There are several potential limitations associated with applying our study to real SCNs that can be easily addressed by extending our current work.

The first potential limitation is the assumption of homogeneous recovery and infection probabilities. In practice, the node risk capacity may be different across nodes in the SCN. By assigning different recovery probabilities and infection probabilities to different nodes, our model could be extended to accommodate networks with various node risk capacities. Moreover, when a company needs to evaluate practical investment decisions for key suppliers with different characteristics, this approach can help with comparing different strategies for improving SCNR. This would also support letting the risk capacity and/or the current state of a given subset of nodes be uncertain (Garvey et al., 2015) and relaxing our assumption that the current state of each node is always known.

The second limitation is that this initial work focuses on non-directed networks and doesn't consider different supply chain tiers. Risk can propagate to both the supplier side and the customer side, but the infection probability may vary depending on the direction of the relationship and the particular role that a firm plays in that relationship. To incorporate such variability, therefore, one could extend our model to a directed network and define different infection and recovery probabilities that depend on more specific supply chain configurations of interest. The third limitation of the current model is that we only consider one-time disruptions, even though in reality the SCN may suffer multiple disruptions in a given time period. By incorporating multiple disruptions into our simulation, we could build on the preliminary results discussed here, to further investigate the resilience behavior of networks under different types of real-world scenarios.

There are a number of additional future research efforts that could also be supported by this work. For example, there is an opportunity to more closely investigate the role that immunity plays in SCNR. Based on the assumption of immunity that was made above, network types generally don't have a significant influence on long-term SCNR. Other studies have shown, however, that scale-free networks can increase the level of risk propagation when no immunity is assumed (Basole and Bellamy 2014). In practice, gaining immunity may require additional investment, and firms need to justify if it is worth to do it. Evaluating how immunity influences SCNR can provide insights into related decision making. The second direction is to apply our work to broader types of networks by adopting specific features that make them unique, whether it's the performance indicator or the structure of the network itself. Looking into broader types of network will allow for developing a better understanding of the different ways in which different types of nodes, and the interactions between those nodes, might influence the different characteristics of SCNR.

References

Albet, R, N Jeong, and A L Barabasi. 2000. "Error and Attack Tolerance of Complex Networks (Vol 406, Pg 378, 2000)." *Nature* 406 (6794): 378–82.

Artur Świerczek. 2014. "The Impact of Supply Chain Integration on the 'Snowball Effect' in the Transmission of Disruptions: An Empirical Evaluation of the Model." *International Journal of Production Economics*. https://doi.org/10.1016/j.ijpe.2013.08.010.

Bailey, N.T.J. 1977. "The Mathematical Theory of Infectious Diseases and Its Applications." *Journal of the Royal Statistical Society. Series C (Applied Statistics)* 26 (1): 85–87. https://doi.org/10.1057/jors.1977.92.

Basole, Rahul C., and Marcus A. Bellamy. 2014. "Supply Network Structure, Visibility, and Risk Diffusion: A Computational Approach." *Decision Sciences*. https://doi.org/10.1111/deci.12099.

Blackhurst, J., C. W. Craighead, D. Elkins, and R. B. Handfield. 2005. "An Empirically Derived Agenda of Critical Research Issues for Managing Supply-Chain Disruptions." *International Journal of Production Research*.

Blackhurst, J.a, K.S.b Dunn, and C.W.b Craighead. 2011. "An Empirically Derived Framework of Global Supply Resiliency." *Journal of Business Logistics* 32 (4): 374–91. https://doi.org/10.1111/j.0000-0000.2011.01032.x.

Bode, Christoph, and Stephan M. Wagner. 2015. "Dimensions of Supply Chain Complexity and Their Effects on the Frequency of Supply Chain Disruptions." *Journal of Operations Management* 36: 215–28.

Borgatti, Stephen P., and Xun Li. 2009. "On Social Network Analysis in a Supply Chain Context." *Journal of Supply Chain Management* 45 (2): 5–22. https://doi.org/10.1111/j.1745-493X.2009.03166.x.

Brandon-Jones, E., Squire, B., Autry, C. W., & Petersen, K. J. (2014). A contingent resource-based perspective of supply chain resilience and robustness. *Journal of Supply Chain Management*, 50(3), 55-73. https://doi.org/10.1111/jscm.12050.

Brintrup, Alexandra, Yu Wang, and Ashutosh Tiwari. 2015. "Supply Networks as Complex Systems: A Network-Science-Based Characterization." *IEEE Systems Journal*, 1–12. https://doi.org/10.1109/JSYST.2015.2425137.

Bruneau, Michel, Stephanie E. Chang, Ronald T. Eguchi, George C. Lee, Thomas D. O'Rourke, Andrei M. Reinhorn, Masanobu Shinozuka, Kathleen Tierney, William A. Wallace, and Detlof Von Winterfeldt. 2003. "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities." *Earthquake Spectra*. https://doi.org/10.1193/1.1623497.

Brusset, Xavier, and Christoph Teller. 2017. "Supply Chain Capabilities, Risks, and Resilience." *International Journal of Production Economics*. https://doi.org/10.1016/j.ijpe.2016.09.008.

Business Continuity Institute. 2018. "Supply Chain Resilience 2018 Annual Survey." https://www.thebci.org/uploads/assets/uploaded/c50072bf-df5c-4c98-a5e1876aafb15bd0.pdf.

Büttner, Kathrin, Joachim Krieter, Arne Traulsen, and Imke Traulsen. 2013. "Static Network Analysis of a Pork Supply Chain in Northern Germany-Characterisation of the Potential Spread of Infectious Diseases via Animal Movements." *Preventive Veterinary Medicine* 110 (3–4): 418–28. https://doi.org/10.1016/j.prevetmed.2013.01.008.

Carter, Craig R., Dale S. Rogers, and Thomas Y. Choi. 2015. "Toward the Theory of the Supply Chain." *Journal of Supply Chain Management* 51 (2): 89–97. https://doi.org/10.1111/jscm.12073.

Chaudhuri, Atanu, Samir K. Srivastava, Rajiv K. Srivastava, and Zeenat Parveen. 2016. “Risk Propagation and Its Impact on Performance in Food Processing Supply Chain: A Fuzzy Interpretive Structural Modeling Based Approach.” *Journal of Modelling in Management*. https://doi.org/10.1108/JM2-08-2014-0065.

Choi, Thomas Y., Kevin J. Dooley, and Manus Rungtusanatham. 2001. “Supply Networks and Complex Adaptive Systems: Control versus Emergence.” *Journal of Operations Management* 19 (3): 351–66.

Choi, Thomas Y., and Daniel R. Krause. 2006. “The Supply Base and Its Complexity: Implications for Transaction Costs, Risks, Responsiveness, and Innovation.” *Journal of Operations Management* 24 (5): 637–52. https://doi.org/10.1016/j.jom.2005.07.002.

Choi, Thomas Y., and Zhaohui Wu. 2009. “Triads in Supply Networks: Theorizing Buyer-Supplier-Supplier Relationships.” *Journal of Supply Chain Management*. https://doi.org/10.1111/j.1745-493X.2009.03151.x.

Christopher, Martin, and Helen Peck. 2004. “Building the Resilient Supply Chain.” 15 (2): 1–13.

Craighead, Christopher W., Jennifer Blackhurst, M. Johnny Rungtusanatham, and Robert B. Handfield. 2007. “The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities.” *Decision Sciences* 38: 131–56.

Dolgui, Alexandre, Dmitry Ivanov, and Boris Sokolov. 2018. “Ripple Effect in the Supply Chain: An Analysis and Recent Literature.” *International Journal of Production Research* 56 (1–2): 414–30. https://doi.org/10.1080/00207543.2017.1387680.

Garvey, Myles D., Steven Carnovale, and Sengun Yeniyurt. 2015. “An Analytical Framework for Supply Network Risk Propagation: A Bayesian Network Approach.” *European Journal of Operational Research* 243 (2): 618–27. https://doi.org/10.1016/j.ejor.2014.10.034.

Gatepoint Research. 2012. “Strategies for Managing Supply Chain Disruption.”

Goto, Hayato, Hideki Takayasu, and Misako Takayasu. 2017. “Estimating Risk Propagation between Interacting Firms on Inter-Firm Complex Network.” *PLoS ONE* 12 (10). https://doi.org/10.1371/journal.pone.0185712.

Greimel, Hans. 2016. “How Toyota Applied the Lessons of 2011 Quake.” *Automotive News*, April 25, 2016. http://www.autonews.com/article/20160425/OEM/304259956/how-toyota-applied-the-lessons-of-2011-quake.

Hanaki, Nobuyuki, Alexander Peterhansl, Peter S. Dodds, and Duncan J. Watts. 2007. “Cooperation in Evolving Social Networks.” *Management Science* 53 (7): 1036–50. https://doi.org/10.1287/mnsc.1060.0625.

Holmes, Thomas J. 2011. “The Diffusion of Wal-Mart and Economies of Density.” *Econometrica* 79 (1): 253–302.

Hosseini, Seyedmohsen, Dmitry Ivanov, and Alexandre Dolgui. 2019. “Review of Quantitative Methods for Supply Chain Resilience Analysis.” *Transportation Research Part E: Logistics and Transportation Review*. https://doi.org/10.1016/j.tre.2019.03.001.

HP. 2011. “2011 Annual Report - HP Investor Relations.”

Hua, Zhongsheng, Yanhong Sun, and Xiaoyan Xu. 2011. “Operational Causes of Bankruptcy Propagation in Supply Chain.” *Decision Support Systems*. https://doi.org/10.1016/j.dss.2011.03.007.

Huang, C. Derrick, Ravi S. Behara, and Qing Hu. 2008. “Managing Risk Propagation in Extended Enterprise Networks.” *IT Professional* 10 (4): 14–19. https://doi.org/10.1109/MITP.2008.90.

Intel. 2011. “2011 Annual Report - Intel Corporation.”

Ivanov, Dmitry. 2017. “Simulation-Based Ripple Effect Modelling in the Supply Chain.” *International*

Journal of Production Research 55 (7): 2083–2101. https://doi.org/10.1080/00207543.2016.1275873.

———. 2018a. *Structural Dynamics and Resilience in Supply Chain Risk Management*. https://doi.org/10.1007/978-3-319-69305-7.

———. 2018b. "Supply Chain Risk Management: Bullwhip Effect and Ripple Effect." In *Structural Dynamics and Resilience in Supply Chain Risk Management*, edited by Dmitry Ivanov, 19–44. International Series in Operations Research & Management Science. Cham: Springer International Publishing.

Ivanov, Dmitry, Boris Sokolov, and Alexandre Dolgui. 2014. "The Ripple Effect in Supply Chains: Trade-off 'Efficiency-Flexibility-Resilience' in Disruption Management." *International Journal of Production Research* 52 (7): 2154–72. https://doi.org/10.1080/00207543.2013.858836.

Jalili, Mahdi. 2011. "Error and Attack Tolerance of Small-Worldness in Complex Networks." *Journal of Informetrics* 5 (3): 422–30. https://doi.org/10.1016/j.joi.2011.03.002.

Jüttner, U, and S Maklan. 2011. "Supply Chain Resilience in the Global Financial Crisis: An Empirical Study." *Supply Chain Management* 16 (4): 246–59.

Jüttner, Uta, and Stan Maklan. 2011. "Supply Chain Resilience in the Global Financial Crisis: An Empirical Study." *Supply Chain Management: An International Journal* 16 (4): 246–59. https://doi.org/10.1108/13598541111139062.

Kim, Yusoon, Yi-Su Chen, and Kevin Linderman. 2015. "Supply Network Disruption and Resilience: A Network Structural Perspective." *Journal of Operations Management* 33–34: 43–59.

Kim, Yusoon, Thomas Y. Choi, Tingting Yan, and Kevin Dooley. 2011. "Structural Investigation of Supply Networks: A Social Network Analysis Approach." *Journal of Operations Management* 29 (3): 194–211. https://doi.org/10.1016/j.jom.2010.11.001.

Kleindorfer, Paul R., and Germaine H. Saad. 2005. "Managing Disruption Risks in Supply Chains." *Production and Operations Management* 14 (1): 53–68.

Kristianto, Yohanes, Angappa Gunasekaran, Petri Helo, and Maqsood Sandhu. 2012. "A Decision Support System for Integrating Manufacturing and Product Design into the Reconfiguration of the Supply Chain Networks." *Decision Support Systems* 52 (4): 790–801. https://doi.org/10.1016/j.dss.2011.11.014.

Lambert, Douglas M., Martha C. Cooper, and Janus D. Pagh. 1998. "Supply Chain Management: Implementation Issues and Research Opportunities." *The International Journal of Logistics Management*. https://doi.org/10.1108/09574099810805807.

Li, Yuhong, Christopher W. Zobel, Onur Seref, and Dean Chatfield. 2019. "Network Characteristics and Supply Chain Resilience under Conditions of Risk Propagation." *International Journal of Production Economics*, October, 107529. https://doi.org/10.1016/j.ijpe.2019.107529.

Lytinen, Steven L, and Steven F Railsback. 2012. "The Evolution of Agent-Based Simulation Platforms: A Review of NetLogo 5.0 and ReLogo." *European Meetings on Cybernetics and Systems Research*.

Macdonald, John R., Christopher W. Zobel, Steven A. Melnyk, and Stanley E. Griffis. 2018. "Supply Chain Risk and Resilience: Theory Building through Structured Experiments and Simulation." *International Journal of Production Research*. https://doi.org/10.1080/00207543.2017.1421787.

Mari, Sonia Irshad, Young Hae Lee, and Muhammad Saad Memon. 2015. "Complex Network Theory-Based Approach for Designing Resilient Supply Chain Networks." *International Journal of Logistics Systems and Management* 21 (3): 365. https://doi.org/10.1504/IJLSM.2015.069733.

Melnyk, Steven A., Christopher W. Zobel, John R. MacDonald, and Stanley E. Griffis. 2014. "Making

Sense of Transient Responses in Simulation Studies." *International Journal of Production Research*. https://doi.org/10.1080/00207543.2013.803626.

Nagurney, Anna. 2010. "Optimal Supply Chain Network Design and Redesign at Minimal Total Cost and with Demand Satisfaction." In *International Journal of Production Economics*, 128:200–208.

Nair, Anand, and José M. Vidal. 2011. "Supply Network Topology and Robustness against Disruptions – an Investigation Using Multi-Agent Model." *International Journal of Production Research*.

Orenstein, Penina. 2016. "How Does Supply Network Evolution and Its Topological Structure Impact Supply Chain Performance?" *2016 Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO)*, 562–69. https://doi.org/10.1109/SMRLO.2016.98.

Perera, Supun, Michael G.H. Bell, and Michiel C.J. Bliemer. 2017. "Network Science Approach to Modelling the Topology and Robustness of Supply Chain Networks: A Review and Perspective." *Applied Network Science* 2 (1): 33. https://doi.org/10.1007/s41109-017-0053-0.

Pettit, Timothy J., Keely L. Croxton, and Joseph Fiksel. 2013. "Ensuring Supply Chain Resilience: Development and Implementation of an Assessment Tool." *Journal of Business Logistics* 34 (1): 46–76.

Pettit, Timothy J, Joseph Fiksel, and Keely L Croxton. 2010. "Ensuring Supply Chain Resilience: Development of a Conceptual Framework." *Journal of Business Logistics* 31 (1): 1–21.

Ponomarov, Serhiy Y., and Mary C. Holcomb. 2009. "Understanding the Concept of Supply Chain Resilience." *The International Journal of Logistics Management*.

Rivkin, Jan W., and Nicolaj Siggelkow. 2007. "Patterned Interactions in Complex Systems: Implications for Exploration." *Management Science* 53 (7): 1068–85. https://doi.org/10.1287/mnsc.1060.0626.

Scheibe, Kevin P., and Jennifer Blackhurst. 2017. "Supply Chain Disruption Propagation: A Systemic Risk and Normal Accident Theory Perspective." *International Journal of Production Research*, 2017. https://doi.org/10.1080/00207543.2017.1355123.

Sheffi, Yossi, and James B Rice Jr. 2005. "A Supply Chain View of the Resilient Enterprise." *MIT Sloan Management Review* 47 (1): 41–48.

Simchi-Levi, David, William Schmidt, Yehua Wei, Peter Yun Zhang, Keith Combs, Yao Ge, Oleg Gusikhin, Michael Sanders, and Don Zhang. 2015. "Identifying Risks and Mitigating Disruptions in the Automotive Supply Chain." *Interfaces* 45 (5): 375–90. https://doi.org/10.1287/inte.2015.0804.

Snyder, Lawrence V, and Burcu Atan, Zumbul; Peng, Peng; Rong, Ying; Schmitt, Amanda J; Sinsoysal. 2012. "OR / MS Models for Supply Chain Disruptions : A Review."

Srivastava, Samir K., Atanu Chaudhuri, and Rajiv K. Srivastava. 2015. "Propagation of Risks and Their Impact on Performance in Fresh Food Retail." *International Journal of Logistics Management*. https://doi.org/10.1108/IJLM-02-2014-0032.

Tang, Christopher. 2006. "Robust Strategies for Mitigating Supply Chain Disruptions." *International Journal of Logistics* 9: 33–45.

Thadakamalla, Hari Prasad, Usha Nandini Raghavan, Soundar Kumara, and Réka Albert. 2004. "Survivability of Multiagent-Based Supply Networks: A Topological Perspective." *IEEE Intelligent Systems* 19 (5): 24–31.

Tierney, Kathleen, and Michel Bruneau. 2007. *Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction. TR News.*

Tomlin, Brian. 2006. "On the Value of Mitigation and Contingency Strategies for Managing Supply Chain Disruption Risks." *Management Science*.

Wagner, S M, and N Neshat. 2010. “Assessing the Vulnerability of Supply Chains Using Graph Theory.” *International Journal of Production Economics* 126 (1): 121–29.

Wagner, Stephan M., and Christoph Bode. 2006. “An Empirical Investigation into Supply Chain Vulnerability.” *Journal of Purchasing and Supply Management* 12 (6): 301–12.

Watts, Duncan J., and Steven H. Strogatz. 1998. “Collective Dynamics of ‘Small-World’ Networks.” *Nature* 393 (6684): 440–42. https://doi.org/10.1038/30918.

White, Joseph, and Paul Lienert. 2018. “Ford Says Lost Truck Production Will Hit Second Quarter Earnings.” *Reuters*, 2018.

Wilensky, U. 1999. “NetLogo.” *Center for Connected Learning and ComputerBased Modeling Northwestern University Evanston IL*. http://ccl.northwestern.edu/netlogo/.

Wu, T., J. Blackhurst, and P. O’Grady. 2007. “Methodology for Supply Chain Disruption Analysis.” In *International Journal of Production Research*, 45:1665–82. https://doi.org/10.1080/00207540500362138.

Xia, Yu, and Thomas Li-Ping Tang. 2011. “Sustainability in Supply Chain Management: Suggestions for the Auto Industry.” *Management Decision* 49 (4): 495–512. https://doi.org/10.1108/00251741111126459.

Zhao, Kang, Akhil Kumar, Terry P. Harrison, and John Yen. 2011. “Analyzing the Resilience of Complex Supply Network Topologies Against Random and Targeted Disruptions.” *IEEE Systems Journal*, 2011.

Zhao, Kang, Akhil Kumar, and John Yen. 2011. “Achieving High Robustness in Supply Distribution Networks by Rewiring.” *IEEE Transactions on Engineering Management* 58 (2): 347–62.

Zhao, Kang, Zhiya Zuo, and Jennifer V. Blackhurst. 2019. “Modelling Supply Chain Adaptation for Disruptions: An Empirically Grounded Complex Adaptive Systems Approach.” *Journal of Operations Management*. https://doi.org/10.1002/joom.1009.

Zobel, Christopher W. 2011. “Representing Perceived Tradeoffs in Defining Disaster Resilience.” *Decision Support Systems* 50 (2): 394–403.

———. 2014. “Quantitatively Representing Nonlinear Disaster Recovery.” *Decision Sciences* 45 (6): 1053–82.

Zobel, Christopher W., and Lara Khansa. 2012. “Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks.” *Decision Sciences* 43 (4): 687–710.

———. 2014. “Characterizing Multi-Event Disaster Resilience.” *Computers and Operations Research* 42: 83–94.