Information Sharing in Supply Chains: a review of risks and opportunities using the Systematic Literature Network Analysis (SLNA)

Abstract

Purpose – The purpose of this paper is to identify and discuss the most important research areas on information sharing in supply chains and related risks, taking into account their evolution over time. This paper sheds light on what is happening today and what the trajectories for the future are, with particular respect to the implications for supply chain management.

Design/Methodology/Approach – The dynamic literature review method called Systematic Literature Network Analysis (SLNA) was adopted. It combines the Systematic Literature Review approach and bibliographic network analyses, and it relies on objective measures and algorithms to perform quantitative literature-based detection of emerging topics.

Findings - The focus of the literature seems to be on threats internal to the extended supply chain rather than external attacks, such as viruses, traditionally related to information technology (IT). The main arising risk appears to be the intentional or non-intentional leakage of information. Also, papers analyse the implications for information sharing coming from "soft" factors such as trust and collaboration among supply chain partners. Opportunities are also highlighted and include how information sharing can be leveraged to confront disruptions and increase resilience.

Research limitations/implications – The adopted methodology allows providing an original perspective on the investigated topic, i.e. how information sharing in supply chains and related risks are evolving over time due to the turbulent advances in technology.

Practical implications - Emergent and highly critical risks related to information sharing are highlighted to support the design of supply chain risks strategies. Also, critical areas to the development of "beyond-the-dyad" initiatives to manage information sharing risks emerge. Opportunities coming from information sharing that are less known and exploited by companies are provided.

Originality/value – This study focuses on the supply chain perspective rather than the traditional IT-based view of information sharing. According to this perspective, this study provides a dynamic representation of the literature on the investigated topic. This is an important contribution to the topic of information sharing in supply chains, which is continuously evolving and shaping new supply chain models.

Keywords – information sharing, information risk, supply chain risk, supply chain management, Systematic Literature Network Analysis (SLNA), literature review, citation network, co-word network, burst detection.

This is the accepted version of an article published in Supply Chain Management.

1. Introduction

Supply chains are nowadays increasingly reliant on information sharing, enabled by automation and technologies that have recently emerged and are shaping companies' supply chain models (Kache and Seuring, 2017). In fact, these technologies make the collection and sharing of detailed data and information simpler and faster, and supply chains are increasingly finding themselves operating in a massively connected global environment. Sharing information leads to benefits for companies such as inventory and cost reduction, better tracing and tracking, and optimized capacity utilization (Lofti et al., 2013). At the same time, information sharing implies a more considerable exposure of supply chains to various types of risks called "information risks" (Rajagopal et al., 2017), which have become according to BCI (2016) the most significant business risk. Examples include loss of control of information and malicious attacks such as viruses, worms and other attacks by hackers (Sharma, 2016).

Given this background, where the emergence of new technologies and applications has paralleled the exponential increase of information sharing and related risks, the academic and industrial communities have witnessed a considerable growth of contributions on these topics (Kembro et al., 2014). Therefore, analyses of the existing literature on these critical business areas could be of paramount importance to the advancement of both theory and practice. Previous literature reviews have focused on different aspects related to information sharing in supply chains, such as: Vendor Managed Inventory (VMI) (Govindan, 2013; Ryu, 2016), and Collaborative Planning, Forecasting and Replenishment (CPFR) (Eksoz et al., 2014; Hollmann et al., 2015; Panahifar et al., 2015; Shen and Chan, 2017); problems and solutions related to secure collaboration in global supply chains based on information sharing (Zeng et al., 2012); approaches to coordination of operations planning decisions through minimum exchange of information (Taghipour and Frayret, 2013); benefits of information sharing (Lofti et al., 2013; Kembro and Naslund, 2014); collaborative risk management, where risk information sharing is one of the relevant key capabilities (Friday et al., 2018). Yet, it appears that an overview of information risks and their evolution is missing. Providing such an overview is important to inform what researchers and practitioners can focus on to effectively manage the risks related to information sharing in supply chains. This gap becomes even more evident when the evolutionary aspect of this field is concerned. In fact, previous literature reviews do not provide predictions regarding where this field is directed, which is of great importance for those areas experiencing turbulent changes, such as the one investigated in the present study. Consequently, we aim at complementing the existing studies with our research.

This paper aims to answer the following research question: *What are the most important research areas on information sharing in supply chains and related risks, taking into account their evolution over time?*

Hence, we seek to shed light on what the state of the art is, by highlighting also breakthrough recent studies showing the latest developments of the field and to unveil what the trajectories for the future are, with particular respect to the implications for supply chain management.

To this aim, we adopt the dynamic literature review method called "Systematic Literature Network Analysis (SLNA)" (Colicchia and Strozzi, 2012), which allows for taking into account the evolutionary aspect missing in the previous contributions. This method combines the Systematic Literature Review approach and bibliographic network analyses. Differently from descriptive reviews, SLNA relies on objective measures and algorithms to perform quantitative literature-based detection of emerging topics (Kim et al., 2016), based on the analysis of bibliometric networks of the data retrieved, such as citations and keywords networks.

The remainder of this paper is as follows. Section 2 introduces materials and methods; the results of the first phase of the adopted method are presented in Section 3 (i.e. Systematic Literature Review). Section 4 describes the results of the second phase of the SLNA method (citation network analysis, citation score analysis and keyword analysis). Results are discussed and research directions are identified in Section 5, while Section 6 contains final remarks.

2. Material and methods

The adopted Systematic Literature Network Analysis (SLNA) method combines the Systematic Literature Review (SLR) approach with bibliographic network analysis. It consists of two phases (see Figure 1).

A Systematic Literature Review (SLR) represents the first phase. SLR can be defined as ‘‘a specific methodology that locates existing studies, selects and evaluates contributions, analyses and synthesizes data’’ (Denyer and Tranfield, 2009, p. 671). Such review approaches are aimed at avoiding bias and ensure rigour, replicability and significant findings (Kembro et al., 2014).

The main steps of this methodology are the following (Colicchia and Strozzi, 2012):

1. Scope of the analysis. To formulate the research question and to frame a correct literature review Denyer and Tranfield (2009) proposed the answer to the questions related to Context, Intervention, Mechanism and Outcome (CIMO).
2. Locating studies ("keywords, time, type of documents, language") through appropriate tools (e.g. databases; Ali et al., 2017)
3. Study selection and evaluation with the identification of inclusion criteria (Kembro et al., 2014; Ali et al., 2017).

A set of selected papers will be obtained as a result. The data used in this work were collected from the Scopus database, which is the largest abstract and citation database of peer-reviewed literature: scientific journals, books and conference proceedings, for over 57 million records (https://www.elsevier.com/en-gb/solutions/scopus). The use of ISI Web of Knowledge database was also explored for retrieving papers. However, in our case we found that the number of retrieved works was smaller and these articles were already included in the sample retrieved from Scopus. Hence, we decided to rely on Scopus only.

The second phase of the adopted methodology implies a bibliographic network analysis and visualization, which in this work will produce a citation network and a keywords network.

The Citation Network Analysis (CNA) relies on the list of references of journal articles or other publications outputs. References point to previous works that have influenced a research development. It is assumed that citations represent how the cited work has influenced an author's new study (Zhao and Strotmann 2015). It is widely acknowledged that citations can be a measure of the relevance of publications, despite the fact that papers receiving a considerable amount of citations are not necessarily representative of impactful and world-class research (Dawson et al., 2014). However, it is fair to say that citations alone are not able to represent a field in a flawless way. Papers may be excluded from the analysis because no other works cite them, regardless of the relevance of their content, or they might have received a limited amount of citations because they have been recently published. Therefore, other tools such as the keywords analysis and the citation score analysis can complement and mitigate the mentioned shortcomings.

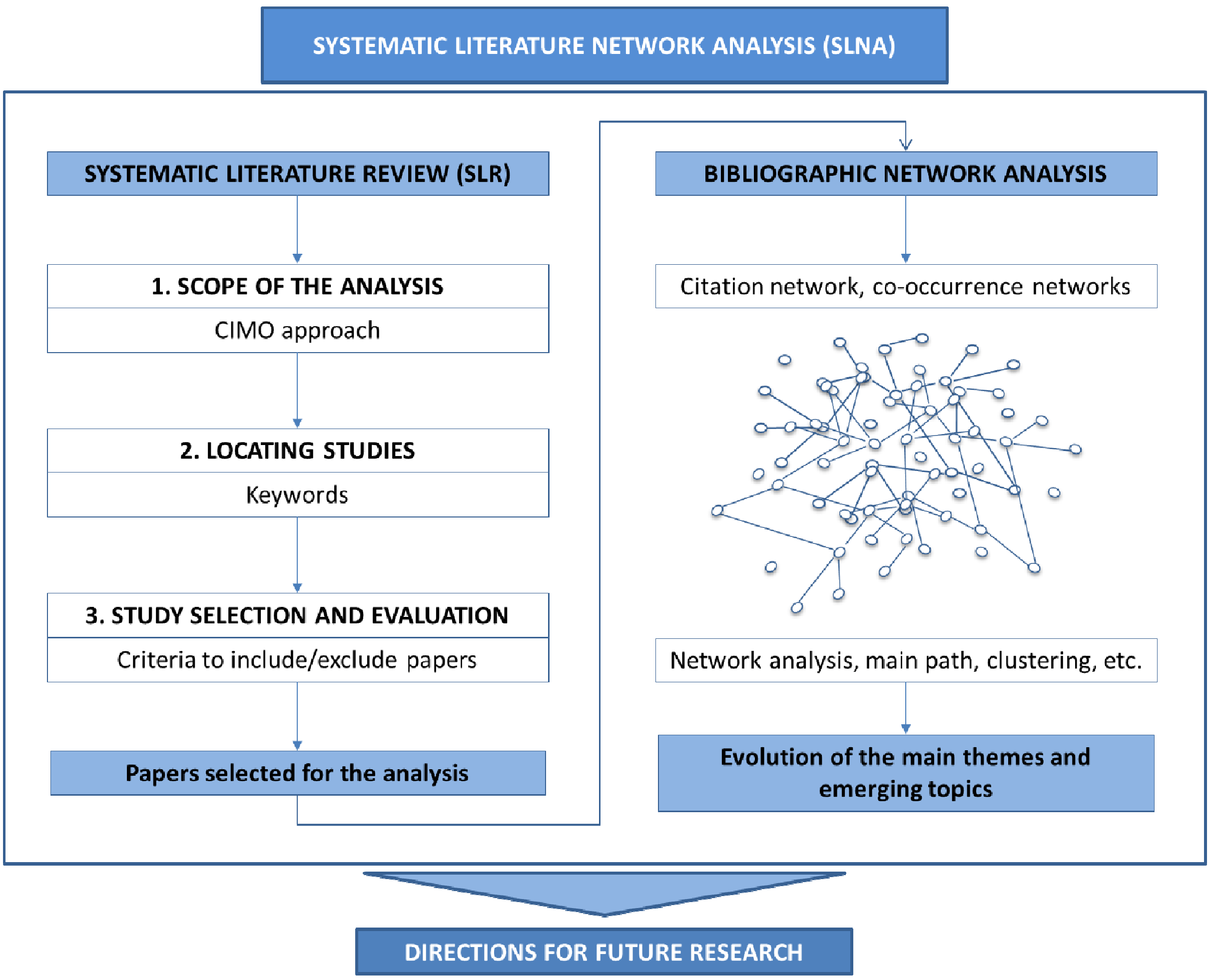


Figure 1. Systematic Literature Network Analysis (SLNA) (Strozzi et al. 2017)

To build bibliographic networks different software packages were adopted. Sci2 Tool (Sci2 Team, 2009) is a modular toolset specifically designed for the study of science and it supports the temporal, geospatial, topical and network analysis and visualization of datasets. Sci2 was used to monitor the temporal evolution of keywords selected by the authors applying the burst detection algorithms. VoS viewer (http://www.vosviewer.com/) is a software package able to analyse bibliometric networks and it was used to produce a keywords network applying the VoS clustering methodology (Van Eck and Waltman 2009) and to build citation networks that can be analysed then using Pajek software. Pajek (De Nooy et al. 2011) is a software package that performs Social Network Analyses and it was used to plot the citation networks.

3. First phase of SLNA methodology: SLR

This section presents the application of the first phase of the adopted methodology to the field under study. The steps represented on the left-hand side of Figure 1 (SLR) are performed and a description of the process is provided.

3.1. Scope of the analysis

This step is essential for avoiding ambiguity in the review through the definition and formulation of the review questions (Ali et al., 2017). Denyer and Tranfield (2009) proposed CIMO-logic to determine the scope of the literature review and formulating the questions. The application of this logic to the field under study is the starting point of our literature review:

- *Context: information sharing.* The emergence of new technologies, applications and paradigms are pushing companies and supply chains to exploit the benefits of information sharing with the aim of reducing operating costs, and improving performance and customer satisfaction.
- *Intervention: information risks.* At the same time, there is an increasing awareness that the massively connected business environment in which companies operate entails a higher exposure to highly critical risks related to the sharing of information throughout the end-to-end supply chain. These risks are called "information risks" and they are gaining increasing importance in today's context.
- *Mechanism: supply chain risk management.* Since information risks can have an effect on all the players of the same supply chain or supply network, effective supply chain risk management strategies and practices need to be devised and shared among supply chain partners.
- *Outcome: increased resilience.* The ability to manage information risks at a supply chain level will allow companies and supply chains to achieve an increased level of resilience, leading to better security and protection from threats and disruptions related to the sharing of information.

3.2. Locating studies

A number of keywords related to the areas identified through the CIMO-logic and to the objective of this study were identified. These were further discussed and refined with a panel of experts from the academic and industrial communities. Keywords selection is critical since it might affect results if different sets of keywords are used. A way to offset this problem (besides the adoption of focus groups to identify keywords leveraging the interaction of different individuals from the academic and industrial communities to reduce personal bias) is the applications of tools to extract information from a set of papers and to discuss outcomes in the light of contextual factors (e.g. governmental actions, published policies). Keywords allow concepts, issues and trends to emerge by applying the various bibliographic analysis tools.

Similarly to other systematic reviews (e.g. Ali et al., 2017; Pereira et al., 2014), the identification of the keywords was performed considering synonymous of information sharing, supply chain, risks related to information sharing in the supply chain and resilience. The concept of “information sharing” is expressed also as “data sharing” and the concept of “supply chain” in the literature sometimes appears as “supply networks”. Regarding the risks related to the sharing of information and resilience the selected keywords were “security”, “risk”, “protection”, “threat”, “disruption”, “resilience”. We obtained the following research string: (“information sharing” OR “data sharing”) AND (“supply chain” OR “supply network”) AND (security OR risk OR protection OR threat OR disruption OR resilience).

3.3. Study selection and evaluation

A number of inclusion criteria were identified to ensure transparency of the process and to evaluate the relevance of the papers to be selected (Table 1).

Table 1. Inclusion criteria for study selection and evaluation (adapted from Ali et al., 2017)

Inclusion criteria	**Rationale**
Published in peer-reviewed journals	Peer-reviewed journals are considered to be of higher quality than non-peer-reviewed articles
Selection of papers without restriction on publication year	Widest possible time window to comply with the purpose of the study, i.e. focus on the evolutionary view of the field
Selection of papers with restriction on the Search Field, i.e. "Title-Abstract-Keywords"	Selected articles present high relevance since keywords must be present in the articles’ title, abstract or keywords
Published in English	English is the dominant language in the field of supply chain management research

First, the search was performed looking for papers published in peer-reviewed scientific journals only. This choice is based on the assumption that by limiting the search to peer-reviewed journals, it is possible to enhance the quality control of search outcomes thanks to the rigorous review process that articles undergo prior to publication in such journals, as argued by Newbert (2007), Pereira et al. (2014) and Ali et al. (2017).

The retrieval of papers from Scopus database ensured that this criterion is met. Additionally, papers were selected without restriction on publication year (i.e. setting ‘All years’ in the Data range field). This allowed taking into account the widest possible time window in accordance with the purpose of this study, i.e. focus on the evolutionary view of the field, without introducing a subjective starting date of the analysis. The identified keywords were used as a search string in Scopus at the beginning of June 2017, resulting in 4,592 articles retrieved. The selection of papers was then refined by restricting the search field to “Title-Abstract-Keywords”. This inclusion criterion ensured that the selected articles presented a high relevance to the field under study (Ali et al., 2017), by requiring the presence of at least three keywords in the articles’ title, keywords or abstract, i.e. one keyword from each area composing our search string (information sharing, supply chain, risk and resilience). This alignment appraisal criterion is effective in making sure that the selected papers are focused on the topic under investigation (Pereira et al., 2014). The refined search led to exclude 4,274 papers, with 318 articles remaining in the sample. Finally, only papers published in English were selected, since English is the dominant language in the field of supply chain management research. This led to obtaining 309 works as a final search outcome, dated from 1998 to 2017.

Table 2 presents the list of top journals ranked according to the number of retrieved papers published in each of them. The top ten journals account for 54 papers, equal to 17.5% of the total retrieved contributions. This shows that the field under study is not dominated by a single category of journals/discipline. Its spectrum spans across a number of different disciplines, including Computer Science, Engineering, Business Management, Decision Science and Social Science.

Table 2. Number of papers by source (top 10)

Journal	**No. of articles**
International Journal of Production Economics	9
International Journal of Production Research	9
European Journal of Operational Research	6
Lecture Notes in Computer Science	6
International Journal of Logistics Systems and Management	5
Applied Mechanics and Materials	4
Computers in Industry	4
Decision Support Systems	4
Supply Chain Management: an International Journal	4
Advanced Materials Research	3
Other	255
TOTAL	**309**

Figure 2 shows the distribution over time of the retrieved papers by publication year. It appears that the field under study experienced a growth in popularity in the last decade, corresponding to the advent of massively connected systems and changes in paradigms, such as Industry 4.0 (Zuehlke, 2010).

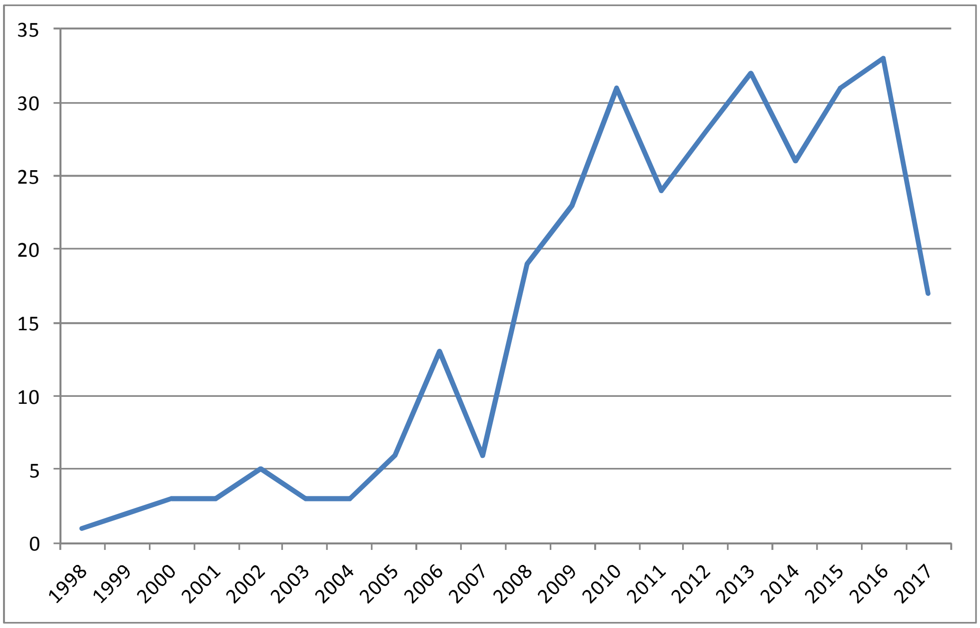


Figure 2. Distribution of articles over time by year of publication (Note: part of 2017 only)

4. Second phase of SLNA methodology: bibliographic network analysis

In this section, we present the application of the second phase of the adopted methodology. In particular, we refer to the right-hand side of Figure 1 and we present the performed bibliometric network analyses.

4.1. Citation Network Analysis (CNA)

A citation network is a network where nodes are papers and links are citations. Arrows link the nodes representing the flow of knowledge from cited papers to citing ones. Figure 3 reports the citation network related to this work. In this network of 309 nodes, 251 nodes are isolated and the remainder is included in connected components, where a connected component is defined as a set of nodes connected by citation links.

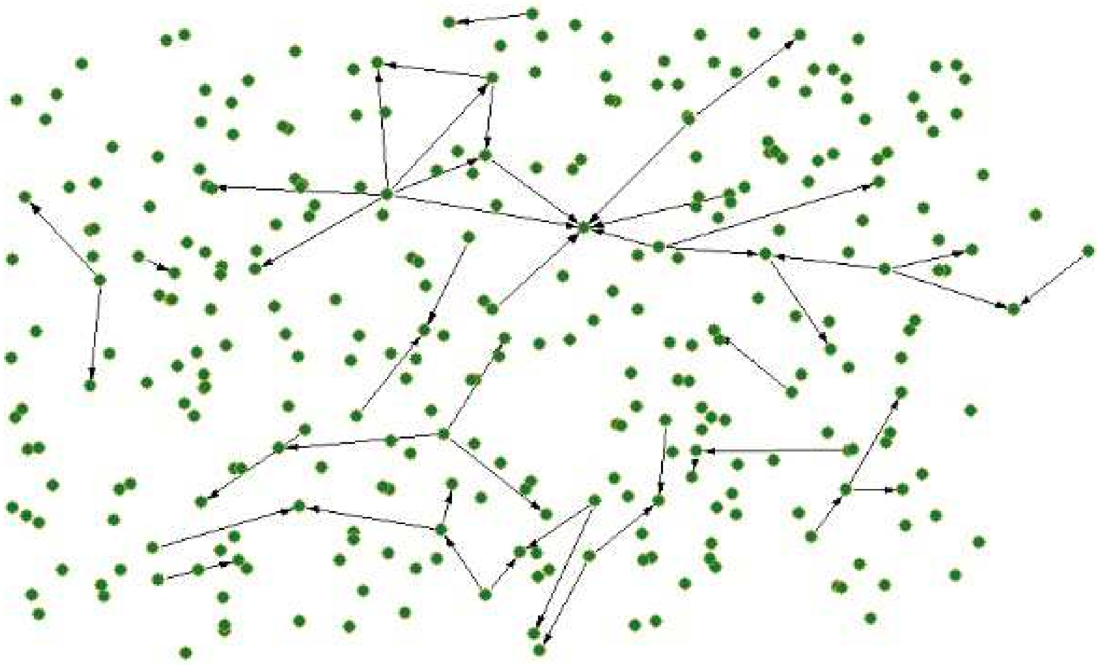


Figure 3. Citation network of 309 papers

Connected components might be composed of a few nodes only or of a large number of nodes, depending on the citation links. As mentioned, CNA is a method based on citations, and as a consequence, it can be applied to connected components only. Therefore, the “isolated” nodes are excluded from this first analysis. The amount of information that can be extracted is larger when connected components are composed of many nodes, hence CNA returns the best results when large connected components are studied (Strozzi et al. 2014). Given these considerations, we focused only on the three biggest connected components of the citation network.

4.1.1. The biggest Connected Component

The biggest component includes 19 nodes. The layout of the nodes represented in Figure 4 is obtained through the Kamada-Kawai algorithm (Kamada and Kawai, 1998) available in the Pajek software package. This algorithm is force-directed and it aims to reduce the edge crossing in a graph taking into account the weights of the various links. This algorithm can be used to visualise the nodes that are connected by stronger links near to each other to detect correlated works, and consequently the main emerging themes.

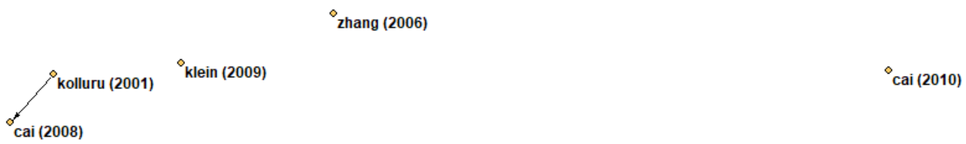
It is also possible to provide a chronological view of the network by showing progressively the appearance of nodes and links among them, which emerge over time. Figure 4-a contains the papers belonging to the biggest connected component published up to 2010 and related citations. Figure 4-b shows the evolution of the component up to 2015, while Figure 4-c shows the complete biggest connected component with all the retrieved papers up to 2017.

In Figure 4-a it is possible to notice that papers start to focus on themes relevant to information sharing but in a disconnected fashion, i.e. architectures for information sharing, effects of information sharing on performance, and enabling factors.
The first theme has been addressed by focusing on securing the architectures for information sharing. This happens through the development of appropriate design frameworks, scalable and interoperable depending on different data sharing needs and security levels (Kolluru and Meredith, 2001) or through the analysis of possible threats and attacks in a supply chain leading to the identification of technologies for securing information sharing (Zhang and Li, 2006). As mentioned, other papers study the positive relationship between information sharing and financial and operational performance (Klein and Rai, 2009). The financial and operational performance is affected by the norms of internet information sharing, which drive the inter-organizational internet communication practices, and are in turn significantly impacted by the perceived internet security risks (Cai and Jun, 2008). Finally, investigations on the enabling factors that can facilitate information sharing start to appear. Institutional forces, including legal protection, government support and interpersonal relationships, are investigated by Cai et al. (2010) within the Chinese context. In particular, while legal protection seems not to have any significant effect, interpersonal relationships (guanxi) directly affect information sharing and government support affects both information sharing and collaborative planning.
In Figure 4-b, papers and themes start to connect. A considerable number of studies appearing up to 2015 start to investigate the risks related to the sharing of information in the supply chain and connected solutions. In particular, the main risk seems to be information leakage, which can be defined as the unintentional disclosure of confidential information to unauthorized parties that may cause the loss of competitive advantage (Zhang et al., 2011). Information leakage protection is traditionally based on two assumptions, i.e. what information is confidential is well known, and confidential information will not be revealed. According to Zhang et al. (2011), these assumptions become unrealistic when inferences are present in supply chains. This means that confidential information can be leaked not only through the so-called "direct leakage", i.e. when confidential information is mistakenly shared, but also in the form of inferences, i.e. when confidential information can be inferred from other shared information, apparently non-confidential. Mitigation approaches are explored to avoid the risk caused by sensitive knowledge leakage through inferences when sharing data in a collaborative relationship (Zhang et al., 2012; Le et al., 2013). The issue of information leakage has been tackled also in the context of global supply chain design. In the context of secure collaboration in a global environment, information leakage risk in a supply chain is related to infrastructure, information, agreement, and confidence (Zeng et al., 2012). In the considered time window, solutions related to information technology, network communications security systems and software applications have been investigated (Wang, 2012; Manzouri et al., 2013). These include cryptography to ensure secure collaboration (Pibernik et al., 2011), applied client-controlled encryption principles in the cloud environment (Kerschbaum, 2014), and secure computation techniques to reduce the risk of information leakage without

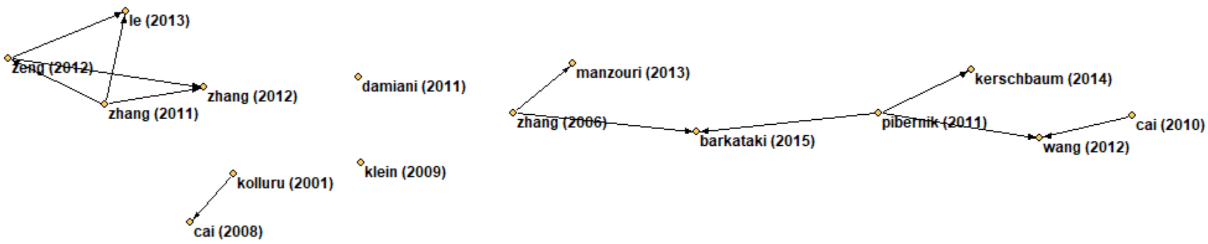
compromising supply chain normal operations (Damiani et al., 2011). In addition, alternative managerial approaches to protection from information leakage start to emerge. These can be based on different levels of trust (strong, weak, none) affecting the design of business processes that enable secure information sharing in a supply chain (Barkataki and Zeineddine, 2015). The consequent “secrecy level”, i.e. the ability to avoid the unwanted exchange of information from suppliers to purchasers, is measured through metrics such as confidentiality, anonymity, privacy, verifiability, non-repudiation.

In Figure 4-c the whole biggest connected component is reported. The additional papers continue the debate on the issue of information leakage risk and related solutions. It emerges that it is first important to identify sensitive knowledge, to be isolated and removed to avoid risk of intentional or unintentional information leakage; then to evaluate residual risks in terms of impacts of information sharing on company’s revenues and performance; to analyse their causes (natural and human factors); and finally to create managerial mitigation approaches (contain, control, contract and cultivate) (Sharma and Routroy, 2016; Tan et al., 2016). In addition, papers further develop the investigation of the importance of trust and interpersonal relationships in the management of risks related to information sharing. Interpersonal relationships and trust play a vital role in facilitating cooperation and information sharing in supply chains (Tran et al., 2016). Affective trust (honesty, mutual understanding, credibility, respect and compliance) and trust in the competence (knowledge/technique, commitment in the relationship) are both necessary to maintain an on-going relationship with partners. Trust leads to a reduction of the bullwhip effect when supply chain management practices involving information sharing are applied (e.g. Vendor Managed Inventory, Collaborative Planning Forecasting and Replenishment, Sales and Operations Planning). However, the lack of affective trust prevents the relationship from developing (De Almeida et al., 2017).

a)



b)



c)

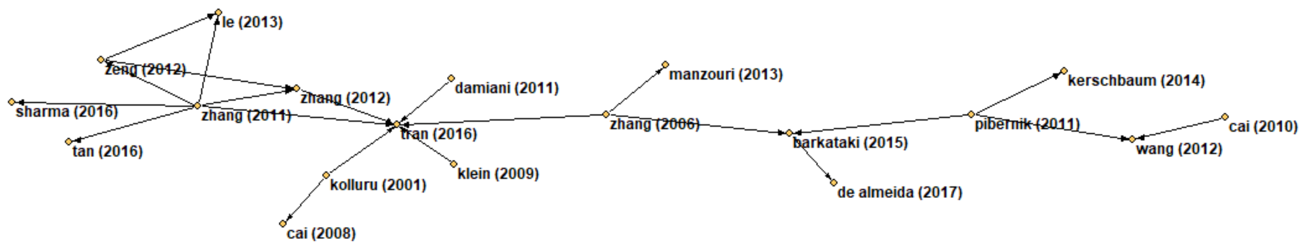


Figure 4. First biggest connected component of the citation network: a) papers up to 2010; b) papers up to 2015; c) complete connected component.

4.1.2. Second and third connected components

In Figure 5-a the second connected component is presented. All the papers of this component deal with information sharing and supply chain disruptions. They consider information sharing as a leverage to allow supply chains to recover and improve their level of resilience. The authors of the papers address this issue from the perspective of simulation studies on one hand and from the perspective of contractual power and risk-sharing contracts on the other. Wakolbinger and Cruz (2011) capture the effect of strategic information sharing on supply chain disruption risk and costs. By developing a model and using numerical examples, they conclude that there is no strong relationship between information sharing alone and risk on a specific level of a supply chain. A stronger relationship is detected when information sharing is combined with other factors, such as contractual power or sharing-risks contracts.

Building on the results of this paper, two main branches stem in this component, as mentioned. One branch contains papers that show how information sharing allows the recovering of a supply chain experiencing disruptions, through the development of simulation models. In particular, Samvedi and Jain (2012) simulate the effect of sharing the forecasting information on supply chain performance during disruptions, giving insights on how to make supply chains more resilient. Costantino et al. (2013) prove the positive effect of information sharing on reducing the Bullwhip Effect in a supply chain. Subsequently, Costantino et al. (2014) propose and test a new replenishment policy based on information sharing and compare it with an Order-Up-To Policy in a four-echelon supply chain. Their results show that information sharing can lead to a stable supply chain performance by reducing the effects of a disruption on inventory and ordering patterns. Tao et al. (2016) quantify the benefits of information sharing on the resilience of a supply chain, by testing three different levels of information sharing in the supply chain (ranging from no-sharing to complete-sharing). The second branch of this component is related to information sharing and risk contracts to protect the supply chain against disruptions and prevent incidents. Jeong (2012) considers the design of a risk-sharing contract in a manufacturer-retailer relationship, and Egri (2013) further investigates how both parties in the relationship should not attempt to achieve higher profits on their own, but they should look at the common interest of the supply chain. Han et al. (2014) investigate the relationship between information sharing and perceived risks in a two-echelon supply chain. They propose a model to study trust issues between a retailer and a supplier, in an information sharing process that involves the transmission of forecasted demand to the supplier and the set-up of a contract to mitigate the perceived risks.

The papers of the third component in Figure 5-b are focused on the value of information sharing and risk propagation mechanisms in complex supply chains, i.e. where manifold layers, suppliers, customers, and products are concerned. In this context, the value of information sharing might depend on the stage of the supply chain where the focal company operates. Firms, especially those that are upstream in the supply chain, may face a significant risk of over-estimating the value of information sharing if they ignore product substitution, demand correlation, and partial information sharing effects (Ganesh et al., 2008; Ganesh et al., 2014). In order to achieve supply chain-wide benefits, it is important to analyse incentives to share information in supply chains because different firms may have different levels of willingness to share information. Among these incentives, the literature analyses the mechanisms of risk propagation in complex supply chains, which encourage companies to share information as a way to better prepare organizations to devise effective risk mitigation strategies. Lou et al. (2016) analyse an incentive mechanism for sharing information based on principal-agent theory for a multi-retailer supply chain. Xu et al (2016) evaluate risk propagation because of information sharing in a multi-sourcing supply chain network.

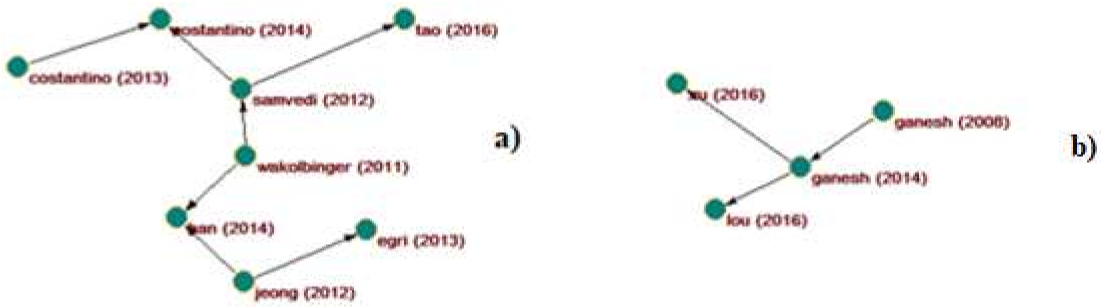


Figure 5. Second and third connected components

4.2. Citation score analysis

The performed citation network analysis on the connected components does not take into account isolated papers because they are not connected through citations to other works. Hence, in order to include in the analysis also these papers, additional bibliometric analyses were performed, i.e. Citation Score Analysis, presented in this section, and the Author Keywords Analysis that will be described in Section 4.3.

Given the relevance of recent evolutions of the topic under investigation, we decided to identify among the set of 309 retrieved papers potential breakthrough recent studies, which represent promising scientific contributions on the subject, showing the latest developments of the field. In order to do this, we performed a ranking of the papers according to the number of citations received in the Scopus database in 2016, divided by their lifespan (i.e. the number of years since publication). This allows identifying those papers that are gaining considerable attention from the scientific community in recent times. Table 3 reports the results of the performed ranking. Some of the identified papers were already discussed above, since they belong to the connected components (i.e. Cai et al., 2010; Ganesh et al., 2014; Klein and Rai, 2009; Wakolbinger and Cruz, 2011).

Four additional papers were identified through this analysis. Brandon-Jones et al. (2014) quantify, through a survey study, the impact of information sharing and supply chain connectivity on visibility, and in turn the impact of visibility on supply chain robustness and resilience. Increased visibility positively affects in a significant way both supply chain resilience and robustness, especially when complexity in the supply side is high, i.e. a large number of suppliers, changing levels of reliability of suppliers, and geographical dispersion of suppliers. The paper of Chae (2015) analyse tweets on hashtag #supplychain. The authors discover that supply chain tweets are also used for information sharing with supply chain partners, or for communicating with stakeholders. This paper investigates a new mechanism for sharing information across the supply chain, through the use of social media. As a result, social media and big data analytics may increase supply chain visibility. Another important finding is that, since the advent of social media, companies are not in full control of the quantity and type of information shared through this mechanism. Nowadays information sharing is not anymore a choice but it is an inevitable consequence of the emergence of Social Networks. Consequently, Big Data Analytics play an increasingly critical role in the analysis of complex communication structures and in sharing information. Speier et al. (2011) examine the threats of potential disruptions on supply chains and propose information sharing among effective mitigation strategies. In the paper of Ha et al. (2011) the effect of trust on logistics efficiency and supply chain collaboration is measured. They analyse the impact on three types of collaboration: joint decision making, information sharing, and benefit/risk sharing.

The papers identified through the Citation Score Analysis and included in Table 3 suggest that literature on information sharing is progressively taking into account the context of modern supply chains and their features, such as complexity (Brandon-Jones et al., 2014), global reach in multi-layer configurations (Ganesh et al., 2014) and interconnectedness among companies and with the institutional environment (Cai et al., 2010). In this context, the literature suggests that a positive relationship exists between information sharing along the supply chain and performance (Klein and Rai, 2009). This relationship is mediated by visibility (Brandon-Jones et al., 2014), enhanced by trust and collaboration mechanisms (Ha et al., 2011), and new technologies such as social media and big data analytics (Chae, 2015). The effect on performance is not related only to financial and operational measures, but the literature also discusses the opportunity to leverage information sharing as a mechanism to manage disruptions in complex modern supply chains (Wakolbinger and Cruz, 2011), and in turn to increase supply chain resilience and robustness (Speier et al. 2011; Brandon-Jones et al., 2014).

Table 3 - Ranking of the top papers in accordance with the citations received in 2016 divided by the number of years since publication.

rank	Publication Year	Authors	Journal Title	<2013	2013	2014	2015	2016	Cit 2016/pubb Years	Part of connected components
1	2014	Brandon-Jones et al.	Journal of Supply Chain Management	0	0	3	11	18	9	
2	2015	Chae	International Journal of Production Economics	0	0	0	1	16	8	
3	2010	Cai et al.	Journal of Operations Management	19	27	26	26	32	5,3	x
4	2014	Ganesh et al.	Decision Support Systems	0	0	3	5	10	5	x
5	2011	Speier et al.	Journal of Operations Management	1	9	16	16	16	3,2	
6	2009	Klein and Rai	MIS Quarterly: Management Information Systems	45	34	35	26	21	3	x
7	2011	Ha et al.	International Journal of Operations and Production Management	7	9	17	22	12	2	
8	2011	Wakolbinger and Cruz	International Journal of Production Research	4	10	9	13	12	2	x

4.3. Author Keywords analysis

The analysis on the author keywords can help in detecting main research areas and research trends extracted from all papers included in a citation network. Basing on Ding et al. (2001), we studied the keywords of the whole set of works retrieved.

4.3.1. Co-occurrence analysis of Authors' keywords

To perform an analysis of the authors' keywords, it necessary to build a co-occurrence (or co-word) network (Callon, 1991). In the present paper, the co-occurrence network nodes are the authors' keywords of the 309 papers and the weight of the links correspond to the number of times that words appear together in the same papers. This analysis is based on the assumption that the authors' keywords of a paper adequately represent the content or the connection of a paper to the theme under investigation. Many co-occurrences around the same word (or pairs of words) may symbolise a research theme, and this can also reveal patterns and trends in a certain field of research (Ding et al., 2001).

We first extracted the authors' keywords of the 309 papers; second, we normalized the keywords, i.e. the text was separated into token words, normalized in lowercase, the "s" at the end of words was deleted, the dots from acronyms removed, the stop words deleted. In this way, we built a "co-word" network, composed of all keywords appearing together for at least five times (i.e. the default value).

The VOSviewer software package (Van Eck and Waltman, 2010) was used to perform the analysis of the co-occurrence keywords network. This package implements the VOS (*Visualization Of Similarities)* clustering technique. VOSviewer identifies the location of items in a map by minimizing a function depending on a similarity measure (*ASij*) between items defined as:

$$AS_{ij} = \frac{c_{ij}}{c_i c_j} \tag{1}$$

where *cij* is the measure of the co-occurrence of keywords *i* and *j* in the same document and *ci* and *cj* are the expected number of co-occurrences of *i* and *j*, with the assumption that the co-occurrences of *i* and *j* are independent from a statistical viewpoint.

Research trajectories using author keywords

Four clusters of keywords were built and analysed (Figure 6). The results are obtained analysing the author keywords of the 309 papers. In Table 4 the number of occurrences of each keyword in the four clusters is reported. Since this represents the number of publications in the sample of selected papers using the keywords, this table provides an additional view of the contribution of the papers to the development of the field.

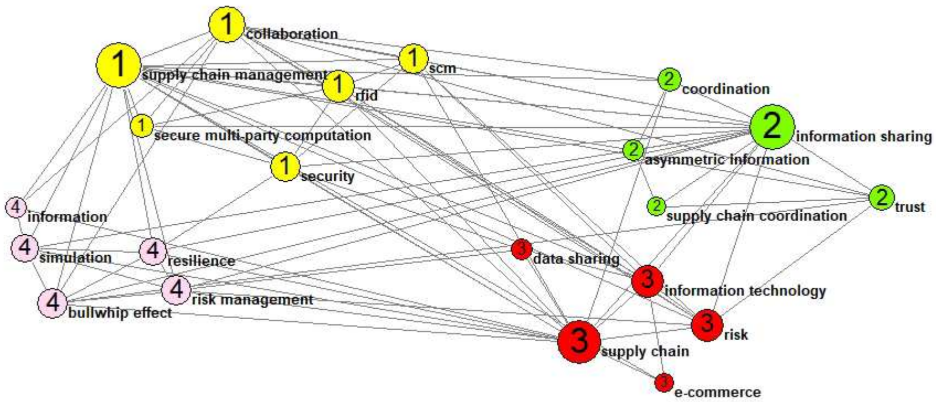


Figure 6. Co-occurrence network of author keywords.

Table 4. Number of occurrences of each keyword included in the Clusters

Cluster	Keyword	Number of Occurrences
1	supply chain management	54
	Rfid	18
	collaboration	9
	Security	9
	scm	6
	secure multi-party computation	5
2	information sharing	75
	Trust	7
	coordination	7
	asymmetric information	7
	supply chain coordination	5
3	supply chain	54
	Risk	10
	information technology	8
	data sharing	5
	e-commerce	5
4	bullwhip effect	14
	risk management	13
	simulation	9
	resilience	6
	information	5

Cluster 1: Protection of Supply Chains from internal threats

Cluster 1 deals with the issue of protection of supply chains from risks coming mainly from threats internal to the supply chain. The focus on internal threats relates to the appearance of keywords such as "Secure Multi-Party Computation (MPC)" and "security", which highlight the importance of techniques to ensure secure information sharing in the supply chain. MPC is a subfield of cryptography, which has the aim to create methods for parties to ensure a secure collaboration and process information while keeping identities private (Kerschbaum et al., 2010). In contrast with cryptography, MPC focuses on threats internal to the supply chain, in other words within the system of participants, and not on the wider external environment. The main goal is to define a protocol to ensure the privacy and correctness of the shared information (Deitos and Kerschbaum, 2009). Interestingly, MPC is closely linked to the issue of security, which traditionally is focused on external threats (viruses, hackers, etc.) to avoid information leakage and enhance protection of the internal side of the supply chain as well. MPC might reconcile data sharing with the privacy concerns but it requires the collaboration of all parties involved (Pibernik et al., 2011; Kerschbaum, 2014). In fact, organizations are required not only to update their protection mechanisms to the most recent standards but also to collaborate with their supply chain partners to integrate protection mechanisms and ensure that the same security standards and protection policies are adopted (Bhargava et al., 2013). In fact, the keywords "collaboration" and "Supply Chain Management" confirm the importance of information sharing and collaborative approaches in the supply chain. This can happen also through the use of technology, as shown by the keyword "RFID", i.e. Radio Frequency Identification, which is a technology that enables collection and sharing of information (Lin, 2009; Kapoor et al., 2009). Although the RFID technology has been widely accepted by the manufacturing sectors, there are still many issues regarding its security and privacy, connected to the potential risk that sensitive information can be disclosed when sharing RFID data with other companies. MPC represents a solution to address this concern in a collaborative supply chain management environment, as discussed by Kerschbaum et al. (2010).

Cluster 2: Asymmetric Information in the supply chain

The second cluster is focused on the concept of "asymmetric information", as shown by the related emerging keyword, which means that one of the parties in a relationship has a larger amount and/or better quality information than the other(s) (Agrell et al., 2004). Some works acknowledge that this imbalance can jeopardize the success of the relationship and ultimately sub-optimal supply chain performance, and discuss ways for overcoming this problem. Among these, the establishment of "trust" in the supply chain is seen as a vital factor. In fact, increased trust can lead disadvantaged parties to accept to a certain level the existence of information asymmetry; trust can also enhance supply chain coordination and consequently reduce the level of information asymmetry (Kim et al., 2011). This is confirmed by the presence of the keywords "trust" and "supply chain coordination". Another solution to operate in the presence of asymmetric information is represented by the set up of appropriate contracts among parties. For example, Ozer and Wei (2006) analyse how different contracts between a supplier and a manufacturer, who owns private forecast information, may enhance supply chain coordination by affecting decisions on production capacity reservation and management. Other contributions discuss the role of revenue/profit sharing contracts in improving the level of truthful information shared across the supply chain (Wang and Wang, 2014; Heese and Kemahlıoglu-Ziya, 2016). Interestingly, Heese and Kemahlıoglu-Ziya (2016) debate also how voluntary information asymmetry can be leveraged in a supplier-retailer relationship for increasing the performance of the entire supply chain when a retailer withholding private information exerts sales efforts. Similarly, Zhou et al. (2012) simulate through a model the benefits of asymmetric information between a supplier and a retailer for improving supply chain profits, when marketing efforts are exerted to influence customers' buying behaviour and increase demand.

Cluster 3: Technology for data sharing and e-commerce

This cluster is focused on the development of information technology supporting, enabling and facilitating the development and diffusion of e-commerce practices, as shown by the keywords "information technology" and "e-commerce". This has implied a growing intensity of data sharing, and the consequent emergence of risks in the supply chain, related to information sharing (as highlighted by the presence of the related keywords "data sharing" and "risk"). The literature discusses these risks and opportunities. For example, Gupta and Narain (2012) investigate the e-procurement processes in India and they address internet security concerns, loss of information sharing, and legal legitimacy as factors to be addressed for building trust in an e-commerce environment. While organisations seem to have the necessary IT infrastructure for e-commerce, the technological barriers mainly related to security concerns and incompatibility still need to be overcome. Arnold et al. (2010) examine the connection between the perception of risk in an e-commerce environment and the commitment and information sharing, where global supply chain partners are involved in a business-to-business relationship. These authors propose that the stronger the risk perception, the smaller the level of commitment and information sharing.

Studies focus also on specific sectors, such as the pharmaceutical, where information technology and digital solutions (such as mobile, RFID, online verification and blockchain) represent an opportunity to fight the global trade of counterfeit medicines and ensure the integrity and security of the global drug supply chain (Mackey and Nayyar, 2017). Stefansson (2002) highlights the opportunities that the advent of the Internet and the concepts of electronic business open up for small and medium enterprises, to effectively and efficiently integrate their logistics operations in the supply chain.

In addition, literature also suggests that a one-size-fits-all approach to the deployment of information technology for e-commerce is not suitable. In fact, there is a need for diversification of IT systems to leverage the benefits of e-commerce and to correctly address the level of environmental and demand uncertainty (Yigitbasioglu, 2010). Four different strategies to develop appropriate data sharing systems in the supply chain are proposed by Wang et al. (2012), and besides information technology, these include the role of the partners, incentives and security systems.

Cluster 4: Information sharing for improved supply chain resilience

This cluster of keywords appears to be focused on the use of tools and techniques such as simulation to map and understand the dynamics of risks related to information sharing and to enhance risk management practices, as shown by the presence of the keywords “simulation” and “risk management”. Simulation approaches include Markov models to integrate forecast, inventory and contract instruments (Gao, 2015), control theory modelling to investigate the disruption mitigation effects of different managerial strategies such as CPFR (Yang and Fan, 2014), and discrete-event simulation models to include risk measures and analysis of profit/losses in a four-stage supply chain (Thierry et al., 2011; Mahmoudi et al., 2006).

Advantages and benefits are also identified, such as the reduction of the bullwhip effect in the supply chain and improved supply chain resilience, as highlighted by the keywords “bullwhip effect” and “resilience”. Literature analyses how information sharing and connectivity may increase the resilience and robustness of complex supply chains (different scale, geographical dispersion, different delivery policies) where the probability of experiencing disruptions is higher (Brandon-Jones et al., 2014), taking into account factors such as trust and behavioural uncertainty (Papadopoulos et al., 2017). While traditionally studies have discussed the benefits of sharing information in the downstream stages of the supply chain, recent works show how sharing information also in the upstream stages proves to be beneficial for disruption management and better resilience (Sarkar and Kumar, 2015). Other contributions have more specifically focused on the value of information sharing for the reduction of the bullwhip effect. Papers discuss the impact of collaborative practices and strategic partnerships in dampening the bullwhip effect and increase the competitiveness of the supply chain (Chao, 2013), the stability of inventory levels (Cannella et al., 2008) and of demand (Shi and Shen, 2013). The bullwhip effect has been traditionally studied with reference to the manufacturing sector. However, some authors have recently focused on specific sectors: Li et al. (2016) present a work on the container shipping market, where they show the benefits of simultaneously incorporating information sharing and risk pooling to handle the bullwhip effect; Somashekhar et al. (2013) investigate the reduction of the bullwhip effect through strategic approaches to inclusive growth in the agricultural sector.

4.3.2. Kleinberg's Burst detection algorithm

The body of knowledge in a certain discipline can be seen as a sequence of topics that appear, grow in importance for a particular period, and then disappear. The emergence of a theme in a stream of documents is flagged by a "burst of activity", with certain elements rising sharply in frequency as the topic emerges. Kleinberg (2003) developed a formal approach to modelling these "bursts", to be identified in an efficient and robust way.

We applied Kleinberg's algorithm to the author keywords of the papers we retrieved. We extracted and pre-processed normalized author keywords adopting the Sci2 software to eliminate the stop-words, upper cases, etc., with a text analysis algorithm. Figure 7 shows the results of the described process in a horizontal bar graph visualisation. In this figure, the x-axis represents time, while the horizontal bars correspond to normalized words. The thickness of each bar is proportional to the "burst" weight. The weight depicts the intensity of the "burst", i.e. how great the change in the word frequency that triggered it. The length of the bars represents the intervals of time in which these "bursts" occurred.

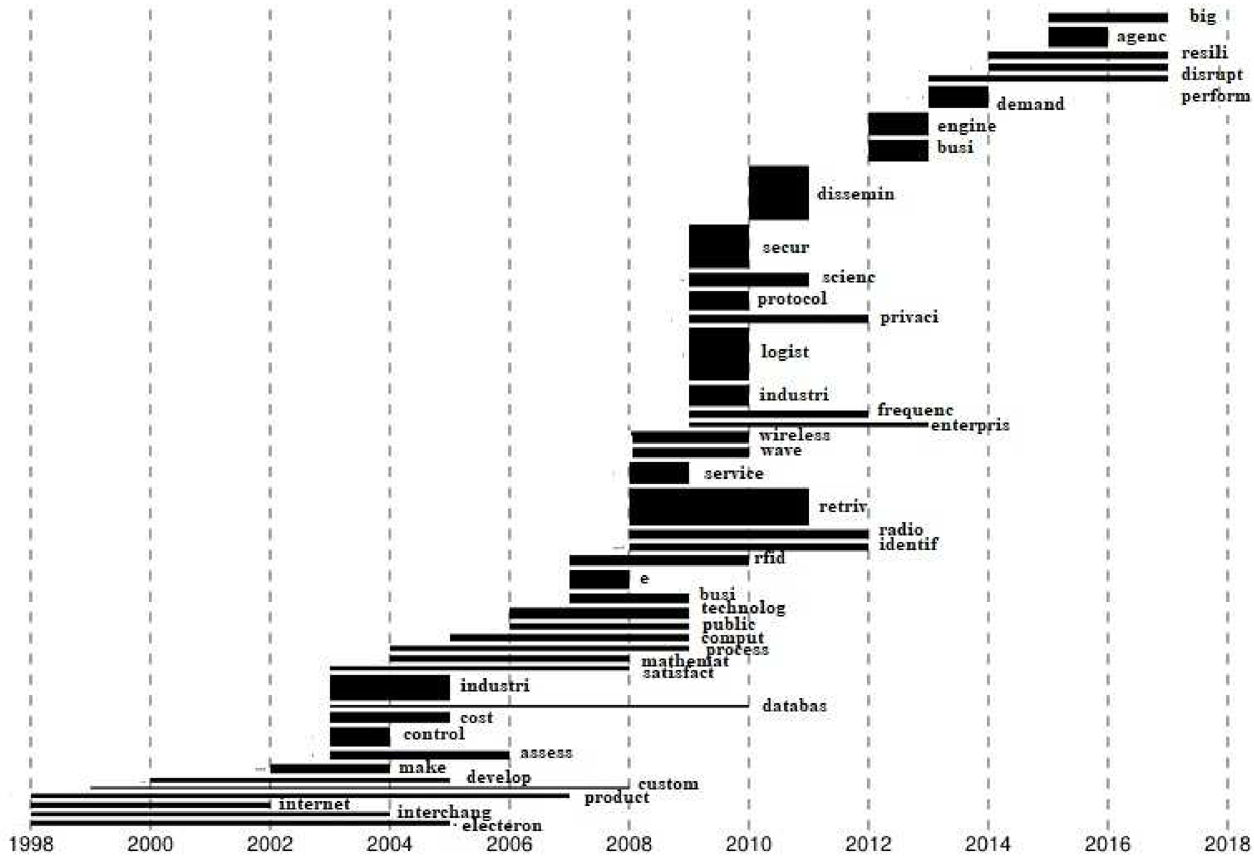


Figure 7. Burst detection Algorithm applied to normalized author keywords.

Around 2009 a considerable number of bursts on security, protocols, logistics, frequency appear, and these seem to be related to an increase in efforts to investigate security problems together with the development of new protocols to ensure privacy. Interestingly, in these years, Germany started to be the promoter of the new paradigm of Industry 4.0 (Zuehlke, 2010), underlining the necessity of information sharing to increase productivity, together with the development of cybersecurity measures. It seems that the adoption of new information technologies such as RFID to collect data brought new risks due to the possibility to share very detailed information about production, and potentially lose control on it. The advantages of information sharing became more and more evident over time, especially when search engines started to allow users to collect more and more data. In fact, in 2012 a burst of the keyword *engine* appeared. This kind of tools, together with social media, allows sharing also information on customers' preferences and demand (demand sensing or demand shaping), which is widely acknowledged as a benefit for supply chain visibility. The burst of the keyword *demand* in 2013 could possibly mean that demand became one of the most interesting types of data to be shared. In 2014 the burst of the keywords *resilience*, *disruption* and *performance* appeared, with papers dealing with the impact of sharing information on resilience, disruption and performance of a supply chain. Very recent trends reflect the rise of interest in big data for information sharing, as shown by the burst of the keyword *big* in 2015. In fact, the diffusion of big data analytics and social networks allow the collection and analysis of a large amount of information through different mechanisms of data sharing.

5. Discussion of the findings and research agenda

By combining the outcomes of the performed analyses, it is possible to provide insights on the main areas investigated by the literature and the research trajectories of the knowledge on information sharing in supply chains, related risks and opportunities. This also allows identifying the main directions for future research to respond to the emerging needs for theory and practice (see Table 5).

1. From an overarching perspective, our analyses showed that the literature on information sharing in a supply chain context has not primarily dealt with those risks associated to the general process of sharing information from an IT/security perspective, such as external threats coming from viruses, hackers, hacktivists, etc. On the other hand, the focus seems to be on threats internal to the supply chain (Deitos and Kerschbaum, 2009; Zhang et al., 2011) but including also stakeholders (Barkataki and Zeineddine, 2015). The main arising risk appears to be the intentional or non-intentional leakage of information (e.g. Tan et al., 2016).
    a. A first factor, as emerging from the work of Chae (2015), is that information sharing in extended supply chains is not even a choice anymore by decision makers and this creates a considerable risk of leakage of information. Companies are everyday challenged by the continuous exchange of information that happens through social media, such as Twitter. If this is, on one hand, an opportunity to access a large amount of data to be analysed through Big Data Analytics (Chae, 2015), on the other hand, it is necessary to explore the "side effects" related to these new ways of sharing information. Further research is needed to investigate the risks and sources of risks connected to information sharing through social media, along with ways to manage them and mechanisms to leverage the opportunities coming from the exchange of information through these platforms.
    b. Another factor that makes information leakage a critical risk is represented by the increasing complexity of modern supply chains, which are multi-layer, multi-supplier, multi-commodity, and multi-channel by nature. As pointed out by the literature, the involvement of manifold players and stakeholders linked by communication channels makes these complex supply chains more vulnerable to leakage of information (e.g. Brandon-Jones et al., 2014; Speier et al., 2011). This is a crucial point since this complexity is reflective of the operating mechanisms and structure of today's real life supply chains. The literature has investigated the dynamics of risk propagation and resilience in these contexts (Papadopoulos et al., 2017; Xu et al., 2015), mainly through simulation studies (e.g. Costantino et al., 2014; Samvedi and Jain, 2012). However, our analyses showed that besides simulation studies, the literature is wanting of real-life applications, identification of best practices and guidelines to manage this type of risk in complex scenarios.

c. Another factor affecting the level of criticality of information leakage along the supply chain is represented by the emergence of the paradigm of Industry 4.0. According to this paradigm, which is built on the concept of integration of cyber-physical systems, production systems and supply chains become more connected, smarter and more efficient, thanks to the combination of Information and Communication systems, technology, data and services in network infrastructures (Zuehlke, 2010). All of this requires an increasing need for sharing a large amount of data and information and consequently, this carries along an increasing level of riskiness in the control of information. This in turns requires an adequate approach to managing cyber and information security and it opens further avenues for future research specifically focused on cyber and information risk management in the information sharing processes within the paradigm of Industry 4.0.

2. As it emerges from our analyses, the literature contains some contributions on potential ways for securing information sharing in supply chains and for confronting the related risks arising. On one side, works have concentrated on the design, development and implementation of IT solutions to increase the level of security in the information sharing processes. These include for example security architectures (Kolluru and Meredith, 2001), existing technologies for securing the transmission of information (Wang et al., 2012; Zhang and Li, 2006) and cryptography (Pibernik et al., 2011). These initiatives are mainly concentrated on managing risks coming from the abovementioned sources external to the supply chain. However, IT solutions are not the major focus of the papers that address the management of the risks related to information sharing in a supply chain context. In fact, most of the previous research is actually focusing on the "soft" side of the problem. Papers analyse the implications for information sharing among supply chain partners coming from factors such as trust, interpersonal relationships, collaboration and cooperation mechanisms, the management of asymmetric information, governmental support, institutional and contractual environments (e.g. Egri, 2013; Ha, 2011; Han et al., 2014; Heese and Kemahlioglu-Ziya, 2016; Kim et al., 2011). Although these concepts have been already widely discussed in the general supply chain management literature, there is need to deepen the study of all the mentioned issues with reference to the specific context under investigation to provide frameworks of solutions and initiatives that can be applied to tackle the challenges deriving from information sharing in supply chains. Also, as advocated by Trombley (2015), the analysis should focus on the effect of human behaviours on information sharing, e.g. how trust among supply chain partners could lead to underestimation of potential consequences of sharing information in a non-security-compliant way for the entire supply chain. In particular, all these initiatives should imply actions that are not supposed to start and accomplish their mission within the boundaries of the focal company, but rather should extend and embrace the supply chain partners upstream and downstream beyond the dyad.
3. Interestingly, several contributions highlight also the opportunities coming from information sharing in supply chains. It is worthwhile to underline that these opportunities are not only connected to those

traditional benefits of information sharing such as an increased efficiency and effectiveness of supply chain processes, but also to how information sharing itself can be potentially leveraged to reduce the level of risk in the supply chain and to confront disruptions. Information sharing is seen as a tool for supporting decision making during disruption responses, through sharing of experiences among supply chain partners, so that companies can access this knowledge and quickly react to disruptions and create post-incident reports accessible to all supply chain partners (e.g. Samvedi and Jain, 2012; Sarkar and Kumar, 2015). An example of how information sharing can make supply chains more resilient to disruptions is represented by the initiative undertaken in the US by President Barak Obama in 2015. An Executive Order was issued on "Promoting Private Sector Cybersecurity Information Sharing", through the creation of Information Sharing and Analysis Organizations (ISAOs). These are organizations aimed at helping businesses to share information on cyber threats among each other and with the public sector, to raise awareness and build a shared knowledge to empower companies to counteract these threats (PwC, 2016). Further to this, also an increased level of visibility thanks to information sharing contributes to enhancing the level of robustness and resilience of supply chains, especially in the case of complex supply chain structures (Brandon-Jones et al., 2014; Speier et al., 2011). Future research should study, develop and test mechanisms for allowing organizations to exploit the benefits coming from information sharing. Contributions are needed to devise and implement initiatives that should be coupled with risk management actions leading to supply chain strategies and models based on a "wise" use of information sharing, i.e. maximising opportunities and minimizing risks. This could also be extended to policymaking, with particular reference to the impact of governmental actions on the diffusion of information sharing practices, for example through protection measures.

Table 5. Research directions (including examples of specific contributions from the analyses of the SLNA)

	Investigated area		**Relationship with Citation Network Analysis**	**Relationship with Citation Score Analysis**	**Relationship with Author Keywords Analysis**	**Relationship with Burst Detection**	**Future research directions**
1	Main arising risk: information leakage in the extended supply chain	a. New information sharing mechanisms and information technologies		Twitter and social network analysis (Chae, 2015)	**Cluster 3:** data sharing; information technologies	*Big data* from 2015	More analysis of risks and opportunities of social media and other tools for information sharing
		b. Information sharing in Complex Supply Chains: impact on risk and resilience	**Component 2:** impact on risk and resilience **Component 3:** simulation of complex supply chains	Information sharing in complex supply chains (Brandon-Jones et al., 2014; Cai et al., 2010; Ganesh et al., 2014)	**Cluster 4:** resilience, simulation	*Resilience, disruption* from 2014	More analysis of real-life complex supply chains, identification of best practices and guidelines
		c. Information Sharing and "Industry 4.0" paradigm	**Component 1:** Secure protocol encryption		**Cluster 1:** internal threats, RFID, secure multi-party computation	*Rfid* from 2007 *Wireless* from 2008 *Industri* from 2009	More analysis of information sharing in Cyber-physical systems
2	Ways for securing Information sharing: "soft" issues		**Component 1:** risk of information leakage and trust	Trust and collaboration issues in the supply chain (Ha et al., 2011)	**Cluster 1:** collaborative approaches **Cluster 2:** trust, coordination, asymmetric information	*Security* and *protocol* from 2009 (collaboration)	More analysis on the impact of the "soft" issues, including human behaviour, on information sharing
3	Information sharing and related opportunities		**Component 2:** information sharing and recovery from disruptions	Enhanced resilience through visibility (Brandon-Jones et al., 2014; Speier et al., 2011; Wakolbinger and Cruz, 2011)	**Cluster 4:** enhanced resilience, risk management practices	*Demand* from 2013, *Resilience, disruption* from 2014	Study and development of mechanisms (including governmental actions) to exploit the benefits of information sharing

6. Conclusions

This paper presents a Systematic Literature Network Analysis (SLNA), which allows providing an answer to the research question of the study (i.e. What are the most important research areas on information sharing in supply chains and related risks, taking into account their evolution over time?). We have identified three main areas investigated by the literature and discussed how they developed over time to unveil research trajectories, insightful for both theory and practice.

From the theoretical viewpoint, our work offers to the research community an investigation on information sharing in supply chains and related risks from an original perspective, i.e. how these are changing and evolving over time due to the turbulent advances in technology and in a business environment increasingly relying on data and information. This is a particularly important contribution since the topic of information sharing in supply chains is continuously evolving and changing shape - gaining increasing relevance - due to the advent of disruptive technologies that alter the way supply chains operate and interact, in a network of massively connected partners. Our review has highlighted the most important research areas in this field and at the same time has identified research trends and evolutionary directions in the generation of knowledge, which constitute the most recent areas where research is pointing at, but still in need of further development. An additional contribution is represented by the application of the SLNA methodology to the field of information sharing in supply chains and related risks, which can be of benefit to the scientific community to perform systematic literature reviews on different topics based on quantitative bibliometric analyses.

From a practical perspective, the industrial community is informed on the emergent and highly critical risks related to information sharing in supply chains that need to be carefully encapsulated in companies' supply chain risk management strategies. Alongside, this research provides guidance on critical areas that need to be prioritized in the development of actions and "beyond-the-dyad" initiatives to manage risks when sharing information along the chain of supply. Our study also brings to the fore those opportunities coming from information sharing that are less known and exploited by companies. While it is widely acknowledged that information sharing can contribute to better efficiency and effectiveness of supply chain processes, it is less known that, if properly exploited, information sharing can also support risk management and disruption mitigation for creating robust and resilient supply chains. This could further improve the positive perception of supply chain managers towards information sharing in their supply chains, and it could facilitate the emergence of new supply chain strategies and models (including risk management) based on data and information in massively connected networks, enabled by technology.

The approach adopted in this work presents some criticisms. The principal limitation is related to the working principle of citations, which as discussed are not able alone to completely embrace the actual contribution of a research to the literature (Shema, 2013). Furthermore, citations are gathered from databases. In our case, we relied on Scopus, which is a vast and comprehensive collection of scientific publications. However, it does not include the whole of the publications ever produced. A final consideration regards the so-called "Matthew effect", i.e. the rich get richer. Well-known researchers, already receiving a considerable amount of citations, tend to receive more and more citations because their works are highly regarded due to their reputation and popularity.

Notwithstanding the mentioned concerns, the value of this work lies not only in the possibility to visualize and examine citation networks and bibliometric data. In fact, the value lies also in the demonstration of the flexibility of the adopted SLNA methodology, which can be applied to several fields of study to draw insights on the evolution of a discipline to direct future research efforts.

References

Agrell, P.J., Lindroth, R. and Norrman, A., 2004. "Risk, information and incentives in telecom supply chains." *International Journal of Production Economics*, 90(1), 1-16.

Ali, A., Mahfouz, A. and Arisha, A. 2017. "Analysing supply chain resilience: integrating the constructs in a concept mapping framework via a systematic literature review", *Supply Chain Management: An International Journal*, 22(1), 16–39.

Arnold, V., Benford, T., Hampton, C., & Sutton, S. G. 2010. "Competing pressures of risk and absorptive capacity potential on commitment and information sharing in global supply chains". *European Journal of Information Systems*, *19*(2), 134-152.

Bhargava, B., Ranchal, R., Othmane, L, B. 2013, "Secure information sharing in digital supply chains," *2013 3rd IEEE International Advance Computing Conference (IACC)*, Ghaziabad, 2013, 1636-1640.

Brandon-Jones, E., Squire, B., Autry, C.W. and Petersen, K.J., 2014. "A contingent resource-based perspective of supply chain resilience and robustness". *Journal of Supply Chain Management*, *50*(3), pp.55-73.

Brin, S. and L. Page. 2012. "Reprint of: The anatomy of a large-scale hyper textual web search engine." *Computer networks*, *56*(18): 3825-3833.

Callon, M., J.P. Courtial and F. Laville. 1991. "Co-word analysis as a tool for describing the network of interactions between basic and technological research: The case of polymer chemistry." *Scientometrics*, *22*(1): 155-205.

Cannella, S., Ciancimino, E., & Marquez, A. C. (2008). "Capacity constrained supply chains: a simulation study". *International Journal of Simulation and Process Modelling*, *4*(2), 139-147.

Chae, B.K., 2015. "Insights from hashtag# supplychain and Twitter Analytics: Considering Twitter and Twitter data for supply chain practice and research". *International Journal of Production Economics*, *165*, pp.247-259.

Chao, Y.F., 2013. "The Bullwhip Effect in Supply Chain and Countermeasures". *Advanced Materials Research* (711), 799-804.

Colicchia, C. and F. Strozzi. 2012. "Supply chain risk management: a new methodology for a systematic literature review." *Supply Chain Management: An International Journal*, *17*(4): 403-418.

Dawson, S., Gasevic, D., Siemens, G. and S. Joksimovic. 2014. "Current state and future trends: a citation network analysis of the learning analytics field." In *Proceedings of the Fourth International Conference on Learning Analytics And Knowledge, March 2014* (pp. 231-240), Indianapolis, Indiana, USA. ACM: New York.

De Nooy, W., A. Mrvar and V. Batagelj. 2011. *Exploratory social network analysis with Pajek* (Vol. 27). Cambridge University Press.

Deitos, R. and Kerschbaum, F., 2009. "Parallelizing secure linear programming". *Concurrency and Computation: Practice and Experience*, 21(10), 1321-1350.

Denyer, D. and D. Tranfield. 2009. Producing a systematic review., in Buchanan, D., and Bryman, A. "Eds.", The Sage Handbook of Organizational Research Methods, Sage Publications, London, 671-89.

Ding, Y., G.G. Chowdhury and S. Foo. 2001. "Bibliometric cartography of information retrieval research by using co-word analysis." *Information processing & management*, *37*(6): 817-842.

Eksoz, C., Mansouri, S.A. and Bourlakis, M. 2014. "Collaborative forecasting in the food supply chain: A conceptual framework". *International Journal of Production Economics*, 158, 120-135.

Friday, D., Ryan, S., Sridharan, R. and Collins, D. 2018. "Collaborative risk management: a systematic literature review". *International Journal of Physical Distribution & Logistics Management*, 48(3), 231-253.

Gao, L. 2015. "Collaborative forecasting, inventory hedging and contract coordination in dynamic supply risk management". *European Journal of Operational Research*, 245(1), 133-145.

Govindan, K. 2013. "Vendor-managed inventory: a review based on dimensions". *International Journal of Production Research*, 51(13), 3808-3835.

GS1. 2016. The GS1 US Visibility framework. White paper, available at http://www.gs1greece.org/DNLfiles/srvNhelp/GS1_SupplyChainVisibility_WhitePaper.pdf

Gupta, M., & Narain, R. 2012. "A study on usage of IT and its implications on e-procurement in Indian organisations". *International Journal of Business Information Systems*, *10*(2), 222-244.

Ha, B.C., Park, Y.K. and Cho, S., 2011. "Suppliers' affective trust and trust in competency in buyers: Its effect on collaboration and logistics efficiency". *International Journal of Operations & Production Management*, *31*(1), pp.56-77.

Heese, H.S. and Kemahlıoğlu-Ziya, E. 2016. "Don't ask, don't tell: Sharing revenues with a dishonest retailer". *European Journal of Operational Research*, 248(2), 580-592.

Hollmann, R.S., Scavarda, L.F. and Tavares Thomé, A.M. 2015. "Collaborative planning, forecasting and replenishment: a literature review". *International Journal of Productivity and Performance Management*, 64(7), 971-993.

Kache, F. and Seuring, S. (2017). "Challenges and opportunities of digital information at the intersection of big data analytics and supply chain management". *International Journal of Operations & Production Management*, 37(1), pp.10-36.

Kajikawa, Y., Ohno, J., Takeda, Y., Matsushima, K. and Komiyama, H., 2007. "Creating an academic landscape of sustainability science: an analysis of the citation network". *Sustainability Science*, *2*(2), pp.221-231.

Kamada, T. and Kawai S. 1998. "An algorithm for drawing general undirected graphs". *Information Processing Letters*, 31, 7-15.

Kapoor, G., Zhou, W., & Piramuthu, S. 2009. "Challenges associated with RFID tag implementations in supply chains". *European Journal of Information Systems*, *18*(6), 526-533.

Kembro, J., Selviaridis, K. and Näslund, D. (2014), “Theoretical perspectives on information sharing in supply chains: a systematic literature review and conceptual framework”, *Supply Chain Management: An International Journal*, Vol. 19 No. 5/6, pp. 609–625.

Kembro, J. and Näslund, D. 2014. "Information sharing in supply chains, myth or reality? A critical analysis of empirical literature". *International Journal of Physical Distribution & Logistics Management*, 44(3), 179-200.

Kerschbaum, F., Oertel, N., & Weiss Ferreira Chaves, L. 2010. “Privacy-preserving computation of benchmarks on item-level data using RFID”. In *Proceedings of the third ACM conference on Wireless network security*, 105-110.

Kim, K. K., Lee, H., & Park, Y. J. 2011. “Interorganizational information systems asymmetry and supply chain performance”. In *Information Science and Service Science (NISS), 2011 5th International Conference on New Trends in* Vol. 2, 388-393.

Kim, S., C. Colicchia, and D. Menachof. 2016. “Ethical Sourcing: An Analysis of the Literature and Implications for Future Research.” *Journal of Business Ethics*, doi:10.1007/s10551-016-3266-8.

Kleinberg, J., 2003. “Burst and hierarchical structure in streams.” *Data Mining and Knowledge Discovery, 7*(4): 373-397.

Lee, H.L., and Whang, S. 2000. “Information sharing in a supply chain.” *International Journal of Manufacturing Technology and Management*, 1(1), pp.79-93.

Li, S., Chen, J., Liao, Y. and Shi, Y., 2016. “The impact of information sharing and risk pooling on bullwhip effect avoiding in container shipping markets”. *International Journal of Shipping and Transport Logistics*, 8(4), 406-424.

Lin, L. C. 2009. “An integrated framework for the development of radio frequency identification technology in the logistics and supply chain management”. *Computers & Industrial Engineering*, *57*(3), 832-842.

Lotfi, Z., Mukhtar, M., Sahran, S. and Zadeh, A.T., 2013. “Information sharing in supply chain management”. *Procedia Technology*, *11*, pp.298-304.

Mackey, T.K. and Nayyar, G., 2017. “A review of existing and emerging digital technologies to combat the global trade in fake medicines”. *Expert opinion on drug safety*, 16(5), 587-602.

Mahmoudi, J., Lamothe, J., Thierry, C. 2006. “Risk analysis for cooperation policie s benefits in reducing the bullwhip effect”. *IFAC Proceedings Volumes*, 12(1), 6-12.

Newbert, S.L. 2007. “Empirical research on the resource based view of the firm: an assessment and suggestions for future research”, *Strategic Management Journal*, 28(2), 121-46.

Özer, Ö. and Wei, W. 2006. “Strategic commitments for an optimal capacity decision under asymmetric forecast information”. *Management science*, 52(8), 1238-1257.

Özer, Ö., & Wei, W. 2006. “Strategic commitments for an optimal capacity decision under asymmetric forecast information”. *Management science, 52*(8), 1238-1257.

Panahifar, F., Heavey, C., Byrne, P. and Fazlollahtabar, H. 2015. "A framework for Collaborative Planning, Forecasting and Replenishment (CPFR): State of the Art". *Journal of Enterprise Information Management*, 28(6), 838-871.

Papadopoulos, T., Gunasekaran, A., Dubey, R., Altay, N., Childe, S.J. and Fosso-Wamba, S., 2017. "The role of Big Data in explaining disaster resilience in supply chains for sustainability". *Journal of Cleaner Production*, 142, 1108-1118.

Pereira, R.C., Christopher, M. and Da Silva, L.A. 2014. "Achieving supply chain resilience: the role of procurement", *Supply Chain Management: An International Journal*, 19(5/6), 626–642.

PwC. 2016. Toward new possibility of threat management, available at: http://www.pwc.com/ee/et/publications/pub/gsiss-report-cybersecurity-privacy-possibilities.pdf

Rajagopal, V., Venkatesana, S.P. and Goh, M. (2017). "Decision-making models for supply chain risk mitigation: A review". *Computers & Industrial Engineering*, 113, pp. 646-682.

Ryu, C.S. 2016. "Review of Vendor Managed Inventory: Investigation on How It Improves Supply Chain Performance". *Journal of Distribution Science*, 14(9), 47-64.

Sarkar, S. and Kumar, S. 2015. "A behavioral experiment on inventory management with supply chain disruption". *International journal of production economics*, 169(2), 169-178.

Sci2 Team. (2009). Science of Science (Sci2) Tool. Indiana University and SciTech Strategies, https://sci2.cns.iu.edu.

Shen B. and Chan, H.L. 2017. "Forecast Information Sharing for Managing Supply Chains in the Big Data Era: Recent Development and Future Research". *Asia-Pacific Journal of Operational Research*, 34(1), 1-26.

Shi, X. and Shen, H., 2013. "The impact of risk aversion on the value of information sharing to dampening the bullwhip effect". *10th International Conference on Service Systems and Service Management*, 375-380.

Somashekhar, I.C., Raju, J.K., Patil, H. 2013. "Reducing bullwhip effect in fresh food vegetable supply chain management: A strategic approach for inclusive growth". *International Journal of Supply Chain Management*, 2 (3), 53-64.

Speier, C., Whipple, J.M., Closs, D.J. and Voss, M.D., 2011. "Global supply chain design considerations: Mitigating product safety and security risks". *Journal of Operations Management*, *29*(7), pp.721-736.

Stadtler, H. and Kilger, C., 2008. "Supply chain management and advanced planning". *Concepts, Models, Software and Case Studies*, *4*.

Stefansson, G. 2002. "Business-to-business data sharing: A source for integration of supply chains". *International journal of production economics*, *75*(1-2), 135-146.

Strozzi, F., Colicchia, C., Creazza, A., & Noè, C. 2017. "Literature review on the 'Smart Factory' concept using bibliometric tools". *International Journal of Production Research*, 55(22), 6572-6591.

Strozzi, F., F. Bono, and E. Gutierrez. 2014. “Bibliometric and Citation Network Analysis: Percolation and Graph Spectral Analysis in the Framework of Wireless Sensor Network Technology.” *EUR Scientific and Technical Research series*. JRC92443.

Taghipour, A. and Frayret, J.M. 2013. “Coordination of operations planning in supply chains: a review”. *International Journal of Business Performance and Supply Chain Modelling*, 5(3).

Thierry, C., Mahmoudi, J. and Lamothe, J., 2011. “Risk analysis for cooperation policies benefits in reducing the bullwhip effect in a telecom supply chain”. *International Journal of Simulation and Process Modelling*, 6(3), 218-227.

Trombley, S. (2015). “Managing your information risk”. *Computer Fraud and Security*, July 2015, pp.5-9.

Van Eck, N. J., and L. Waltman. 2010. “Software survey: VOSviewer, a computer program for bibliometric mapping.” *Scientometrics*, *84*(2): 523-538.

Van Eck, N.J. and L. Waltman. 2009. “How to normalize co-occurrence data? An analysis of some well-known similarity measures.” *Journal of the American Society for Information Science and Technology*, *60*(8): 1635-1651.

Wang, X. and Wang, X., 2014. “Contracting to Share Bilateral Information in Supply Chain”. *In Proceedings of the Seventh International Conference on Management Science and Engineering Management*, Berlin, Heidelberg, 881-892.

Yang, T, and Fan, W. 2016. “Information management strategies and supply chain performance under demand disruptions”. *International Journal of Production Research*, 54(1), 8-27.

Yigitbasioglu, O.,M. 2010. "Information sharing with key suppliers: a transaction cost theory perspective", *International Journal of Physical Distribution & Logistics Management*, 40(7), 550-578.

Zeng, Y., Wang, L., Deng, X., Cao, X. and Khundker, N. 2012. “Secure collaboration in global design and supply chain environment: Problem analysis and literature review.” *Computers in Industry*, 63 (6), 545-556.

Zhao, D. and Strotmann, A. (2015), “Analysis and visualization of citation networks”. *Synthesis Lectures on Information Concepts, Retrieval, and Services*, *7*(1), pp. 1-207.

Zhou, J., Zhao, X., Xue, L. and Gargeya, V. 2012. “Double moral hazard in a supply chain with consumer learning”. *Decision Support Systems*, 54(1), 482-495.

Zuehlke, D., 2010. “SmartFactory—Towards a factory-of-things.” *Annual Reviews in Control 34*(1): 129-138.

Appendix 1 (the full list of 309 retrieved documents is available upon request)

Biggest connected component

Barkataki, S. and Zeineddine, H., 2015. On achieving secure collaboration in supply chains. *Information Systems Frontiers*, *17*(3), pp.691-705.

Cai, S. and Jun, M., 2008. A qualitative study of the relationship between interorganizational internet communication and purchasing performance. *International Journal of Management and Enterprise Development*, *5*(6), pp.683-707.

Cai, S., Jun, M. and Yang, Z., 2010. Implementing supply chain information integration in China: the role of institutional forces and trust. *Journal of Operations Management, 28*(3), pp.257-268.

Damiani, E., Frati, F. and Tchokpon, R., 2011. The role of information sharing in supply chain management: the securescm approach. *International Journal of Innovation and Technology Management*, *8*(03), pp.455-467.*hnology*, *39*(2), pp.201-210.

De Almeida, M.M.K., Marins, F.A.S., Salgado, A.M.P., Santos, F.C.A. and da Silva, S.L., 2017. The importance of trust and collaboration between companies to mitigate the bullwhip effect in supply chain management. *Acta Scientiarum. Tec*

Kerschbaum, F., 2014, November. Client-controlled cloud encryption. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1542-1543). ACM.

Klein, R. and Rai, A., 2009. Interfirm strategic information flows in logistics supply chain relationships. *Mis Quarterly*, pp.735-762..

Kolluru, R. and Meredith, P.H., 2001. Security and trust management in supply chains. *Information Management & Computer Security*, *9*(5), pp.233-236.

Le, H.Q., Arch-Int, S., Nguyen, H.X. and Arch-Int, N., 2013. Association rule hiding in risk management for retail supply chain collaboration. *Computers in Industry*, *64*(7), pp.776-784.

Manzouri, M., Ab Rahman, M.N., Nasimi, F. and Arshad, H., 2013. A model for securing sharing information across the supply chain. *American Journal of Applied Sciences*, *10*(3), p.253.

Pibernik, R., Zhang, Y., Kerschbaum, F. and Schröpfer, A., 2011. Secure collaborative supply chain planning and inverse optimization–The JELS model. *European Journal of Operational Research*, *208*(1), pp.75-85.

Sharma, S. and Routroy, S., 2016. Modeling information risk in supply chain using Bayesian networks. *Journal of Enterprise Information Management*, *29*(2), pp.238-254.

Tan, K.H., Wong, W.P. and Chung, L., 2016. Information and knowledge leakage in supply chain. *Information Systems Frontiers*, *18*(3), pp.621-638.

Tran, T.T.H., Childerhouse, P., and Deakins, E., 2016. Supply chain information sharing: challenges and risk mitigation strategies. *Journal of Manufacturing Technology Management, 27*(8), pp.1102-1126.

Wang, X., 2012, October. Research on the construction of supply chain collaboration system based on information sharing. In *Information Management, Innovation Management and Industrial Engineering (ICIII), 2012 International Conference on* (Vol. 1, pp. 469-472). IEEE.

Zeng, Y., Wang, L., Deng, X., Cao, X. and Khundker, N., 2012. Secure collaboration in global design and supply chain environment: Problem analysis and literature review. *Computers in Industry*, *63*(6), pp.545-556.

Zhang, C. and Li, S., 2006. Secure information sharing in internet-based supply chain management systems. *Journal of Computer Information Systems*, *46*(4), pp.18-24.

Zhang, D.Y., Cao, X., Wang, L. and Zeng, Y., 2012. Mitigating the risk of information leakage in a two-level supply chain through optimal supplier selection. *Journal of Intelligent Manufacturing*, *23*(4), pp.1351-1364.

Zhang, D.Y., Zeng, Y., Wang, L., Li, H. and Geng, Y., 2011. Modeling and evaluating information leakage caused by inferences in supply chains. *Computers in Industry*, *62*(3), pp.351-363.

Second and third biggest connected components

Costantino, F., Di Gravio, G., Shaban, A. and Tronci, M., 2013. Information sharing policies based on tokens to improve supply chain performances. *International Journal of Logistics Systems and Management*, *14*(2), pp.133-160.

Costantino, F., Di Gravio, G., Shaban, A. and Tronci, M., 2014. Replenishment policy based on information sharing to mitigate the severity of supply chain disruption. *International Journal of Logistics Systems and Management*, *18*(1), pp.3-23.

Egri, P., 2013. A centralized/decentralized design of a full return contract for a risk-free manufacturer and a risk-neutral retailer under partial information sharing: A discussion. *International Journal of Production Economics*, *141*(1), pp.437-438.

Ganesh, M., Raghunathan, S. and Rajendran, C., 2008. The value of information sharing in a multi-product supply chain with product substitution. *Iie Transactions*, *40*(12), pp.1124-1140.

Ganesh, M., Raghunathan, S. and Rajendran, C., 2014. The value of information sharing in a multi-product, multi-level supply chain: Impact of product substitution, demand correlation, and partial information sharing. *Decision Support Systems*, *58*, pp.79-94.

Han, G., Dong, M. and Sun, Q., 2014. Managing distrust-induced risk with deposit in supply chain contract decisions. *The Scientific World Journal*, *2014*.

Jeong, I.J., 2012. A centralized/decentralized design of a full return contract for a risk-free manufacturer and a risk-neutral retailer under partial information sharing. *International Journal of Production Economics*, *136*(1), pp.110-115.

Lou, Y. and Liu, Z., 2016, June. Research on Incentive Mechanism for Information Sharing in supply Chain with Multi-retailer Participants. In *PACIS*(p. 39).

Samvedi, A. and Jain, V., 2012. Effect of sharing forecast information on the performance of a supply chain experiencing disruptions. *International Journal of Logistics Systems and Management*, *13*(4), pp.509-524.

Tao, Y., Lee, L.H. and Chew, E.P., 2016. Quantifying the Effect of Sharing Information in a Supply Chain Facing Supply Disruptions. *Asia-Pacific Journal of Operational Research*, *33*(04), p.1650029.

Wakolbinger, T. and Cruz, J.M., 2011. Supply chain disruption risk management through strategic information acquisition and sharing and risk-sharing contracts. *International Journal of Production Research*, *49*(13), pp.4063-4084.

Xu, H.Y., Fu, X., Ponnambalam, L., Namatame, A., Yin, X.F. and Goh, R.S.M., 2015, December. A model to evaluate risk propagation considering effect of dynamic risk information sharing and multi-sourcing in supply chain networks. In *Industrial Engineering and Engineering Management (IEEM), 2015 IEEE International Conference on* (pp. 1593-1597). IEEE.