

Supply chain security management: a citation network analysis

Xun Tong*

Faculty of Economics and Business,
University of Groningen,
Nettelbosje 2, 9747 AD Groningen, The Netherlands
Email: x.tong@rug.nl
*Corresponding author

Chris K.Y. Lo

Business Division, Institute of Textiles and Clothing,
The Hong Kong Polytechnic University,
1 Yuk Choi Road, Hung Hom, Kowloon, Hong Kong
Email: tccl@polyu.edu.hk

Kee-hung Lai and T.C.E. Cheng

Faculty of Business,
The Hong Kong Polytechnic University,
11 Yuk Choi Road, Hung Hom, Kowloon, Hong Kong
Email: mike.lai@polyu.edu.hk
Email: edwin.cheng@polyu.edu.hk

Abstract: Security management has become a topical issue in supply chain management (SCM). Researchers are keen to address issues related to the prevention, mitigation, and recovery from security incidents and to the development of security management systems with cost efficiency consideration. This study presents a citation network analysis (CNA) of supply chain security (SCS) by analysing 143 sample SCS articles. Specifically, we conduct a cluster analysis and a main path analysis to identify the research clusters in SCS literature and show knowledge transformation in SCS chronically. We identify four research clusters, which are: 1) SCS conceptualisation and application; 2) security management systems; 3) transportation security; 4) terrorism, and the research gaps in each cluster are discussed in this review. This study helps reveal the current trend in SCS management research and suggest potential research directions for future study in SCS.

Keywords: supply chain security; SCS; literature review; citation network analysis; CNA; main path analysis; MPA.

Reference to this paper should be made as follows: Tong, X., Lo, C.K.Y., Lai, K-h. and Cheng, T.C.E. (2019) 'Supply chain security management: a citation network analysis', *Int. J. Shipping and Transport Logistics*, Vol. 11, No. 6, pp.508–532.

Biographical notes: Xun Tong is an Assistant Professor in the Department of Operations, University of Groningen, The Netherlands. His research interests include socially responsible supply chain management, projects management, and systems dynamics. He published papers in the *Journal of Operations Management* and *International Journal of Production Economics*.

Chris K.Y. Lo is an Associate Professor at the Institute of Textiles and Clothing of Hong Kong Polytechnic University. His research interests are sustainability, quality management, and innovations. He has published in *Manufacturing and Service Operations Management*, *Organization Science*, *International Journal of Production Economics*, *Journal of Operations Management*, etc.

Kee-hung Lai (Mike Lai) is a Professor and the Director of Shipping Research Centre at The Hong Kong Polytechnic University with a research interest in logistics and shipping management. He is Editor-in-Chief of the *Journal of Shipping and Trade* and has co-authored seven books and 140 research papers in related areas with an h-index of 59 according to the Google Scholar Citation.

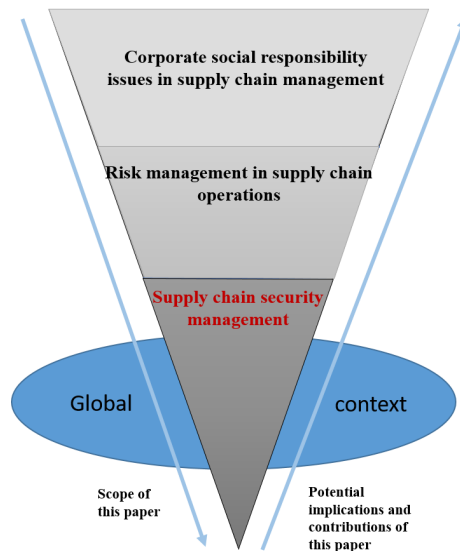
T.C. Edwin Cheng is the Dean of PolyU Business School, Fung Yiu King – Wing Hang Bank Professor in Business Administration, and Chair Professor of Management at The Hong Kong Polytechnic University. His research interests are in operations management and operations research. He has published over 700 papers and co-authored 14 books according to Google Scholar, he has received over 32,000 citations and his h-index is 86.

1 Introduction

Corporate social responsibility (CSR) issues have been emphasised in recent supply chain management, which promote an environmentally friendly production/operations and wellbeing of employees at work (Jamali and Neville, 2011). Some scholars categorise operational risk management into the regime of CSR management because the objectives of risk prevention/mitigate are in line with CSR goals (Godfrey et al., 2009). Lewis (2003) defined operational risk as “the potential for an operation to generate negative consequences for various external and internal stakeholders.” Operational risks are caused by variations/disruptions that affect materials, products, and information flows in the supply chain (Jüttner et al., 2003). Operations managers continuously seek management innovations to mitigate such risks along with other types of risk occurring in the global supply chain management such as uncertain currency exchange rate and political instability (Meixell and Gargeya, 2005). Supply chain risk exists everywhere including ports, factories, warehouses, etc. (Fang et al., 2013; Yip, 2008) across the global supply chain. Supply chain risk management spans various aspects, such as problems of coordination between supply and demand, labour strikes, natural disasters, etc. For example, prior studies propose the emergency logistics distribution approach to counter the risks of disasters in a limited time frame (Sheu, 2007) and provide possible solutions to disaster relief operations in the context of humanitarian logistics. Mathematical models have been used to find optimal solutions for managing the risks of outsourcing by considering time, quality, and costs (Zhu, 2016), as well as the risks of hub disruption in a biomass supply chain (Marufuzzaman et al., 2014). The above-mentioned risks could be a result of randomised events, such as earthquakes, and it

does not matter whether there is an agent (e.g., smugglers and terrorists) actively intervening the operations. In addition, among various risks inherent in the global supply chain, security breaches frequently occur to cause damages to supply chain partners and stakeholders (e.g., customers). This article focuses on one specific type of CSR issue [i.e., supply chain security (SCS)] in global supply chain management endeavouring to provide managerial and theoretical insights for the broader risk and CSR management in OR and OM literature with a focus on SCS. Figure 1 gives the scope and potential contribution of this article.

Figure 1 The scope and potential contributions of this paper (see online version for colours)



SCS management, as defined by Closs (2008), concerns “the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction (WMD) into the supply chain.” In general, security management emphasises formulating strategies to prevent or mitigate the adverse consequences caused by security breaches. SCS management, compared with operational risk management in supply chain context, places an extra emphasis on the active disruptions caused by unknown agents, who might harbour illegitimate motives for their actions. To develop a secure supply chain, operations managers must evaluate the vulnerability of each operations process in order to minimise the exposure of their operations procedures to unknown third-party agents. For example, since the terrorist attack on the New York World Trade Centre in 2001, global logistics security has been tightened up (e.g., imposition of additional inspections and deployment of advanced security technologies).

Piracy not only causes huge losses in cargoes, but also diminishes the quality logistics services because ships need to be re-routed to avoid further losses. Cargoes may contain WMD, illegal drugs, and prohibited chemicals. Moreover, logistics and inventory facilities are liable for damages, which render raw materials and products in inventory or in transit unavailable. The risks associated with such incidents will compromise the performance of the supply chain and undermine customer satisfaction. Security issues in supply chains are relatively under-explored compared with the broader risk management research (Lu et al., 2017), leaving plentiful opportunities for future research. Recently, to promote better management of SCS issues, governments and trading organisations have initiated various SCS management programs, such as Customs-Trade Partnership against Terrorism (C-TPAT), Authorized Economic Operator (AEO), and the International Ship and Port Facility Security (ISPS) code for all the organisations in a supply chain. Supply chain partners (e.g., overseas suppliers and transport carriers) voluntarily or are mandated to implement security practices to showcase their commitment to security management (Autry and Bobbitt, 2008; Sarathy, 2006). The adopter organisations use these security standards to guard themselves against loss caused by undesirable security incidents. In view of the growing importance of security management in OM and OR, we review the published security management studies in the OM literature with the following objectives:

- 1 visualise and analyse the knowledge structure and content of existing SCS studies
- 2 propose possible future research opportunities on SCS issues based on the analysis of the existing literature.

We use the citation network analysis (CNA) to conduct the review. CNA has the advantage of providing an objective identification of the research domains (Pilkington and Meredith, 2009) which are the clusters in the citation network. The number of clusters is determined by the optimised modularity index (Colicchia and Strozzi, 2012; Fan et al., 2014). On the other hand, the main path analysis (MPA) conducted in each cluster helps understand knowledge structure in each sub-area of SCS topic, which can be used to sum up the previous research activities and suggest future research directions.

A brief review of SCS literature below helps understand the current trend under SCS research. Researchers had paid scant attention to SCS issues prior to the terrorist attack in the US on 11 September 2001. For example, before the attack, homeland security management received limited attention in SCM research. The tightened security control across borders after the attack has prompted researchers and practitioners to investigate how SCS management could help improve the security and performance of global supply chains that are vulnerable to increasing and widespread risks of disruption. Roughly, research studies on security issues in SCM include:

- 1 empirical investigations regarding the impact of security practices implementation (Chang et al., 2014; Lu and Koufteros, 2014)
- 2 mathematical modelling to optimise management systems incorporating security considerations (Bakshi and Gans, 2010)
- 3 theoretical exposition of pertinent issues such as security enhancement and security breach prevention/recovery (Melnyk et al., 2013).

This classification is based on the methodologies (i.e., empirical, analytical modelling, and conceptual) adopted, which depends on subjective criteria for classification. In addition, the broad classification above is inadequate in covering all the security-related issues in SCM. For example, it does not cover studies on technological adoption for SCS, which has emerged as a popular management approach for mitigating security breaches. Moreover, given the continuing growth in globalised production and outsourcing activities, firms emphasise coordination among supply chain partners for managing SCS. Hence, the perspective of traditional security management that mainly focuses on facility, personnel, or warehouse security (the traditional view generally focuses more on the within-organisation security issues) is inadequate to embrace the contemporary view of security with a global supply chain focus (which highlights a global perspective where the coordination between organisations in managing SCS is required). Also, a review of security management highlights the risks associated with active agents with illegitimate motives to cause disruptions, which has evolved as a major concern in contemporary supply chain management. Taken together, we demonstrate topical clusters (CNA) and incremental knowledge transformation (MPA) in the following sections, which helps researchers identify future research opportunities in SCS studies by considering the current issues in the SCM context and the limitations of the methodology we employ. In addition to the future research directions suggested at the end of each MPA (see Section 4) we suggest avenues for future research from a broader SCS perspective in Section 5.

The rest of this paper is organised in the following ways. Section 2 introduces the method applied in this study. Section 3 discusses clusters identified through CNA. Section 4 further outlines the knowledge structure of each cluster by using MPA. Finally, Sections 5 and 6 suggest future research directions and a new framework for SCS management, respectively.

2 Methodology

The conventional systematic literature review approach is largely objective but inevitably some decisions are subjective. Decisions on sample papers classification may be biased. Researchers determine the major research domains, based on their knowledge, and thus the quality of the domain classification is largely dependent on their capability. Moreover, the conventional method cannot accurately capture the dynamics of the research trend. To address these concerns, recent OM researchers have adopted the CNA approach to objectively classify the pertinent literature into specific research domains (Fahimnia et al., 2015; Fan et al., 2014).

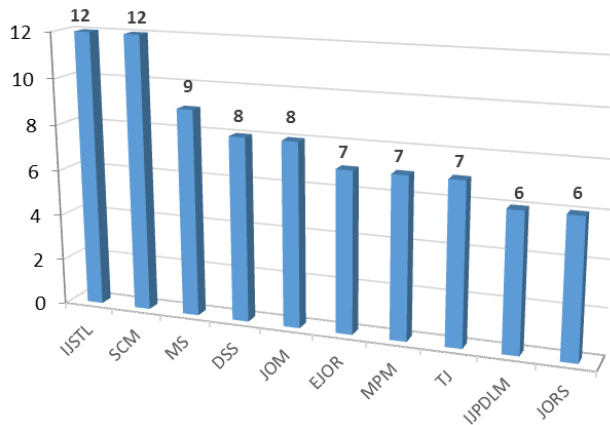
To obtain an initial sample set of SCS-related research papers, we first identified relevant keywords for the literature search in the *Web of Science* (WOS) database. We used the following keywords: 'supply chain', 'security', 'secured', 'management', 'terrorism', 'operation', 'accident', and 'risk'. We also used reasonable combinations of these keywords: 'supply chain AND security', 'secured AND supply chain', 'security AND management', 'operation AND security', 'accident AND management', 'risk AND management', as well as the single words 'terrorism' and 'accident'. Given that SCS is a

relatively new topic, we set a 20-year review period from 1995 to 2015.¹ We limited document types to 'article' and refined the results under *WOS*' categories function by restricting them only to *operations research*, *management science*, and *business*. We identified 257 articles for further analyses. We carefully read each paper and eliminated articles that are outside the research scope (i.e., articles that only contain the above keywords but are irrelevant to SCS studies). Eventually, we collected 143 papers as the sample for further analysis.

Table 1 The top five researchers and their articles' total local citation scores (LCSSs) and global citation scores (GCSs)

Rank	Author	No. of articles published	Total LCSSs/GCSs
1	MD Voss	5	18/57
2	DJ Closs	4	18/57
3	Z Williams	4	13/44
4	TCE Cheng	3	5/126
5	SA Melnyk	3	1/21

Figure 2 Distribution of number of articles published in journals (excluding journals with fewer than six sample articles) (see online version for colours)

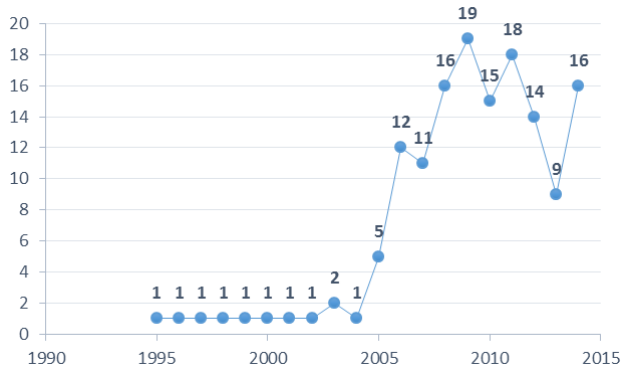


Note: IJSTL = *International Journal of Shipping and Transport Logistics*, SCM = *Supply Chain Management – An International Journal*, MS = *Management Science*, DSS = *Decision Support Systems*, JOM = *Journal of Operations Management*, EJOR = *European Journal of Operations Management*, MPM = *Maritime Policy & Management*, TJ = *Transportation Journal*, IJPDLM = *International Journal of Physical Distribution & Logistics Management*, JORS = *Journal of the Operational Research Society*.

Table 2 The top five contributing organisations/countries and their total LCSs and GCSs

Rank	Organisation	No. of articles	Total LCSs/GCSs	Country	No. of articles	Total LCSs/GCSs
1	Michigan State University	8	19/100	USA	88	173/2,540
2	SUNY Buffalo	6	4/363	China	21	10/290
3	Central Michigan University	5	17/62	UK	15	7/107
4	The Hong Kong Polytechnic University	5	5/153	Canada	7	11/85
5	Purdue University	5	1/36	Australia	4	3/63

We used the statistical software packages *HistCite* and *Gephi*² to conduct the CNA. We first performed a descriptive statistical analysis of the journals downloaded from WOS by using *HistCite*. Tables 1 and 2 and Figures 1 to 5 present the sample articles' top author ranking, contributing organisation/country ranking, distribution by journal, by publication year, by articles' research methodology, and data collection/analysis method, respectively. We used *Gephi*, a powerful tool for providing visualised and interpretative clusters figures, to generate the cluster figures (see Figure 6).

Figure 3 Distribution of number of articles by year (see online version for colours)

We now provide a series of bibliometric analysis on the identified papers including the information of authors, contributing organisations/countries, journals, and publication years. Table 1 reports the five most productive researchers, and their total local citation scores (LCSs) and global citation scores (GCSs). LCS refers to the attention received by other authors within the same research domain (e.g., scholars in OR). GCS indicates how a selected paper has received citations from other research disciplines (e.g., policy research). For example, some sample papers have frequently been cited by administrative policymaking or homeland security research works (e.g., Mueller and Stewart, 2012). Our database shows that the rankings of LCS and GCS are not necessarily consistent. Table 2 shows the top five contributing organisations/countries with respect to LCS and GCS. Michigan State University (organisation) and the USA (country) provide the most contribution to the SCS literature. Figure 1 displays the distribution of publications by

journal. SCS management articles frequently appear in the *International Journal of Shipping and Transport Logistics and Supply Chain Management – An International Journal*, while only a few articles appear in the broader SCM outlets. Figure 2 shows the trend of the SCS related publications, which has experienced a dramatic growth since 2005. This trend implies that increasingly the academia has been paying attention to security management issues. Figure 3 shows the number of papers in terms of the type of article, data collection method, and data analysis method. 78 (54.55%) sample articles adopt the empirical approach, and ten (6.70%) articles use mathematical modelling, 14 (9.79%) articles employ meta-analysis, 25 (17.48%) articles are conceptual works, and 16 (11.19%) articles are literature reviews. Figure 4 shows the data collection methods used: among the 78 empirical papers, 19 (24.36%) use case studies, 31 (39.74%) are survey studies, 20 (25.64%) are interview-based, two (2.56%) use secondary data, and six (7.69%) provide multiple sources of evidence.

Figure 4 Distribution of article types (see online version for colours)

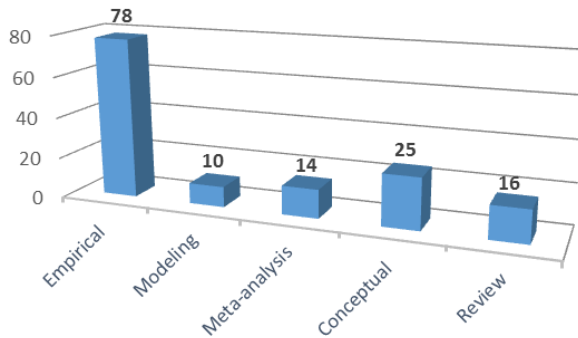
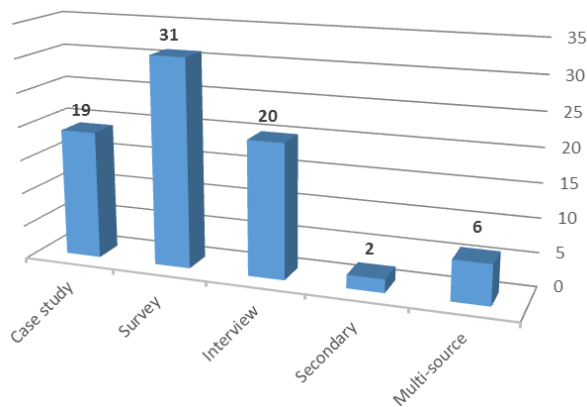


Figure 5 Distribution of data collection method (see online version for colours)



3 Citation network analysis: major research clusters

We use CNA to identify clusters from our sample articles. In any network, a cluster can be identified by maximising the density within a cluster while minimising the connections of nodes between different clusters (Clauset et al., 2004; Radicchi et al., 2004). CNA is based on the concept of ‘edge-betweenness’ (EB). Instead of searching for edges that are central to communities, EB focuses on edges that are ‘between’ communities (less central). This algorithm aims at progressively removing loosely connected edges from a quasi-constructed graph such that a solid community structure (clustered communities) can be finally outlined; see Girvan and Newman (2002). Specifically, we can view a cluster in a citation network as a group of articles that are potentially under the same research topic.

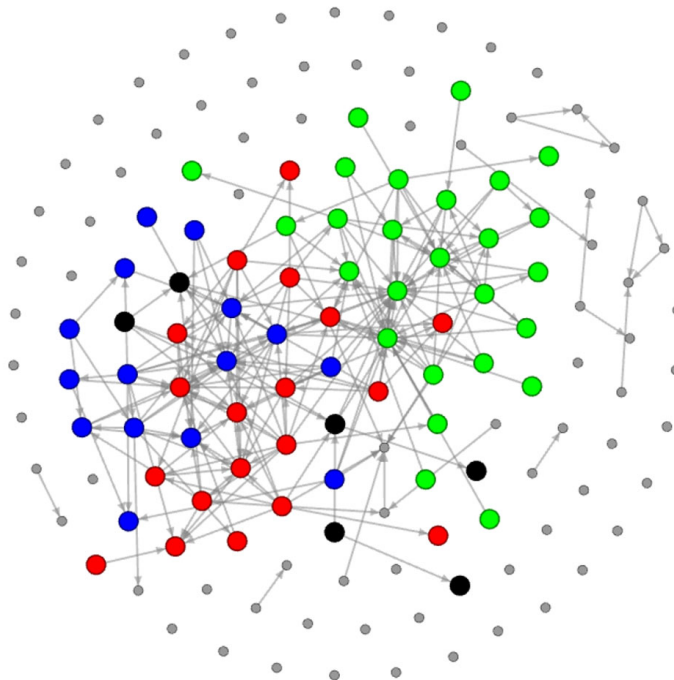
We use the *Gephi* clustering package to determine the number of clusters and classify each node (i.e., article) into its corresponding cluster. A modularity index is needed for optimising the ‘modularity’ of a network by measuring the within-cluster and between-cluster densities. De Meo et al. (2011) proposed the formula below to calculate a network’s modularity Q :

$$Q = \sum_{s=1}^m \left[\frac{l_s}{|E|} - \left(\frac{d_s}{2|E|} \right)^2 \right]$$

where m refers to the number of clusters, s is a cluster, E stands for the total number of edges in a network, l_s is the number of edges between the nodes of a particular cluster s , and d_s represents the sum of degrees of the nodes in the s^{th} cluster. The above formula reflects that in order to maximise the network modularity Q , i.e., to create clusters with high densities within themselves but loosely coupled between one another. Each given cluster should involve the highest possible number of edges, while the network should be divided into several clusters with a total degree as small as possible. Based on the above approach, we obtain four major clusters. The optimal number of clusters is 19 (the Q value is 0.440). However, we find that 15 of the 19 clusters contain only one to three nodes (articles). Given that the numbers of articles in the 15 clusters are very small, we should confirm the creation of the 15 clusters. Labelling these clusters as ‘scattered clusters’, we review the relationships between the nodes in the scattered clusters to avoid omitting any major article that belongs to other major clusters. Figure 5 shows the final four major research domains identified by CNA. We provide a list of the articles under each of the clusters in the Appendix. Table 3 shows that, among the 143 sample articles, 26 papers (18.18%) are related to SCS conceptualisation and application, 19 papers (13.29%) discuss security management systems, 15 papers (10.49%) examine maritime security, and six papers (4.20%) deal with terrorism and other external risk issues. The results also show that 77 papers in our sample do not belong to any cluster. This is attributable to the limitation of CNA as the number of citations from a paper is usually inversely proportional to its year of publication. Recently published papers may have fewer citations, leading to weak connections with papers that may actually contain similar research topics in nature, hence failing to be classified.³

Table 3 The four major research areas identified

Cluster	Research area	No. of articles
1	SCS conceptualisation and application	26
2	Security management systems	19
3	Transportation security	15
4	Terrorism	6

Figure 6 Identifying clusters by using CAN (see online version for colours)

Cluster 1: Green (SCS Conceptualization and Application)

Cluster 2: Red (Security Management Systems)

Cluster 3: Blue (Transportation Security)

Cluster 4: Black (Terrorism)

Notes: 1 – We used the *Gephi* software (*Louvain algorithm*) to determine the optimal number of research clusters. The Q value (modularity index) equals 0.440 and the suggested number of cluster is 19. Small nodes (in gray) represent scattered clusters; 2 – Different colours of nodes refers to different clusters (as indicated in the legend).

4 Main path analysis: the knowledge structure

Clustering a network provides an overview of the literature. However, it cannot chronically capture the incremental development of the knowledge and the transformation of research paradigms. We need to know how an article integrates prior knowledge and leads to new research avenue. It should be noted that the fundamental objective of MPA is not to review the details of the contents in a specific research domain, but to capture the knowledge transformation process and provide possible research opportunities that can be perceived according to the overall research paradigm. Resolving the above problem, the MPA measures the connectivity of articles by searching the nodes (articles) with the highest centrality degree. Articles in the main path are considered critical and pioneering in its research domain. The MPA first calculates the ‘traversal weight’ of each article within a research domain. The traversal weight of an arc or vertex is “the proportion of all paths between *source* (earliest cited article) and *sink* (latest and never being cited) vertices that contain this arc or vertex” (De Nooy et al., 2005). The main path articles are obtained by removing the arcs below a certain level of the traversal weight and eventually articles with greater traversal weights will be included in the main path. Following Fan et al. (2014), we calculate the traversal weight as follows:

$$W_{ij} = TP_{ij} / TBS_j$$

where TP_{ij} represents the total number of citation paths from a particular article i to *sinks* in the network while TBS_j denotes the total number of citation paths between all the articles and *sinks*. We conduct the MPA using the *Pajek 2.05* software.

4.1 Main path analysis for all the sample articles

Figure 6 shows the overall MPA for all the sample articles. Lee and Whang (2005) emphasised the importance of SCS research and introduced how fundamental quality management approaches can address SCS issues. Kleindorfer and Saad (2005)’s security assessment framework suggested how SCS can be prevented by employing mindful strategies in a firm’s supply chain management. Inspired by the above two works, Sarathy (2006) provided a comprehensive review of the relationship between security management and the global supply chain. This conceptual paper provides a holistic view of security management issues in SCM, the impact of security risks, the importance of collaborative relationship between supply chain partners, and the potential research directions.

Based on the conceptual guidance from Sarathy (2006)’s work, Voss et al. (2009a) conducted an empirical study on supplier selection with a security concern in the food supply chain (e.g., under what circumstances do firms compromise production and delivery efficiency for supplier security). Their study revealed that firms with international exposure show stronger security awareness and such awareness improves the firm’s operating performance.

Yang (2011) conducted an in-depth investigation of maritime security issues in view of insufficient attention being paid to maritime security regulations in the literature. Yang (2011) developed maritime security strategies to strengthen cargo security in Taiwan and discussed maritime security initiatives (e.g., 24-hours rule and container security

initiative) with respect to their applications in Taiwan. Furthermore, Yang (2011) employed a bowtie analysis to model accident scenarios by synthesising the causes and impacts of accidents.

Yang and Wei (2013) discussed other security management dimensions, such as facility and cargo management, accident prevention and processing, information management, and partner relationship management, for firm's and customs' security performance. Similarly, Chang et al. (2014) estimated the likelihood of security accidents, relevant consequences, and accident scale by the stochastic dominance method and risk-mapping technique. They provided useful guidance for the customs to identify response strategies to prevent accidents.

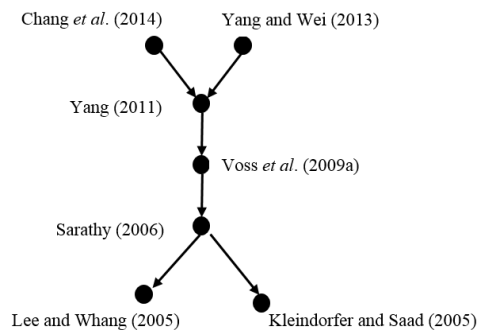
The results of the MPA for all the sample articles suggest that the SCS management domain starts with resembling a relatively natural quality management approach in OM/OR research to guide the SCS research, e.g., Lee and Whang (2005). Progressively, the literature highlights a global perspective in SCS research comprising discussions on the collaboration between partners to mitigate risks (Sarathy, 2006). After that, the research in SCS is investigated in some specific industries such as food processing and maritime shipping industries.

4.2 Cluster 1: SCS conceptualisation and application

SCS conceptualisation and application is the largest research area among the clusters. Figure 7 chronically depicts the knowledge transformation and accumulation in this research area.

Three key research works (Chopra and Sodhi, 2004; Kleindorfer and Saad, 2005; Tomlin, 2006) constitute the foundation of this cluster. Chopra and Sodhi (2004) discussed various factors that may cause security problems and thereby threaten supply chain efficiency. They provided management guidelines to ensure a firm's security performance by minimising the firm's and the firm's partners' potential security accidents. Bakshi and Kleindorfer (2009)'s security framework points out that the emerging SCS concern may arise from 'acts of purposeful agents', e.g., terrorists. The framework consists of self-assessment tools to prevent potential security problems. Bakshi and Kleindorfer (2009) empirically tested and enriched the proposed framework in their study.

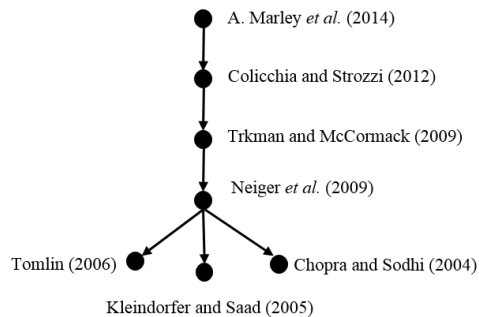
Figure 7 The overall main path for all the sample papers



Tomlin (2006) studied the sourcing problem related to supplier reliability. It was a pioneering work on supplier selection under logistics security and cost restrictions. Tomlin (2006) studied how various supplier characteristics (in particular supplier reliability) and the nature of security breaches affect a firm's strategic decisions on SCS. Based on the three foundation works discussed above, Trkman and McCormack (2009) explored how endogenous uncertainty (market turbulence and technological turbulence) and exogenous uncertainty (continuous risk and discrete events) will affect the likelihood of security disruptions.

Whipple et al. (2009) conducted a literature review of supply chain risk, while SCS was recognised as a key domain for further research. The review also helps practitioners to identify and apply security strategies in their SCM. A. Marley et al. (2014) proposed a theoretical model to study SCS based on the normal accident theory perspective. Normal accident theory implies that accidents are inevitable (normal) when the environment is highly complex or tightly coupled. Accordingly, the authors suggested strategies to prevent SCS accidents by reducing the complexity and decoupling of systems.

Figure 8 The main path for cluster 1 (*SCS conceptualisation and application*)



Given that security research in OM and OR is relatively recent compared with other research realms, e.g., occupational safety, research on SCS is mainly derived from a broader concept of risk management and supply chain disruption research. Therefore, this stream of research mainly focuses on general concepts/frameworks of SCS topics and suffers from the following drawbacks. The articles in the main path of this cluster demonstrate that SCS manager differs from risk management in general due to its “relatively higher level of intentionality (by an agent)” (Lu et al., 2017). This cluster contributes to the SCS literature by highlighting the necessity of separating SCS issues in academic research and practices from the broader risk management research. In view of growing global outsourcing and off-shore manufacturing activities, the above studies provide limited implications because their analyses are restricted to supplier selection with security concerns. Therefore, for future studies on this cluster, a deeper understanding of broader security coordination among various supply chain partners (e.g., suppliers, manufacturers, transport carriers, and end customers) is needed. Also, the security of outsourcing from upstream partners is of great importance to manufacturing firms because if a security problem occurs, manufacturing firms may fail to arrange substitutes, resulting in loss of productivity. Eventually, it will affect downstream service

performance (e.g., on-time delivery). Hence, future studies may investigate how the upstream security management efforts will affect downstream service performance.

4.3 Cluster 2: security management systems

Articles in this cluster are specific to the security management system, comprising SCS management standards or programme initiated by the government, professional organisations (e.g., ISO), and firms. This cluster provides practical insights on the management and implementation of security management systems.

Russell and Saldanha (2003) developed five principles for logistics security management by considering the cost of managing terrorist attacks, complying with government regulations, or adopting a widely accepted standard security certification. Based on a case study, Sheu et al. (2006) confirmed the positive effect of adopting C-TPAT, a popular standard logistics security certification, on the improvement of international supply chain collaboration.

Autry and Bobbitt (2008) conceptualised SCS orientation, which is “a firm-level orientation representing the firm’s collective attention to supply chain security management.” SCS orientation of an organisation helps distinguish the concept of SCS from general supply chain risk. They showed the importance and timeliness of considering security management as an independent and critical research area that should not be restricted to the realm of supply chain risks or supply chain disruptions.

Williams et al. (2008) classified the security management literature with respect to security risk mitigation and security performance enhancement into four categories, namely intra-organisational, inter-organisational, a combination of the two, and ignoring both. They clarified the terminologies used in SCS research and comprehensively reviewed the strategies and practices that organisations adopt in managing SCS.

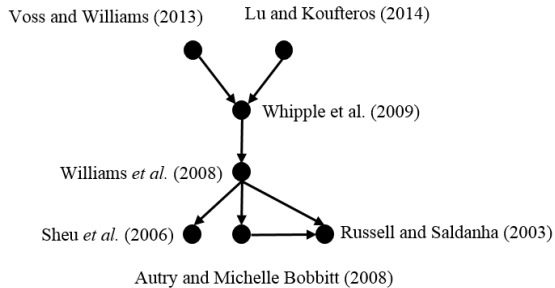
Whipple et al. (2009) empirically investigated the security performance differences between global and local food companies. The results indicate that global food firms and local firms differ significantly in security performance outcomes because a more complex operational environment (i.e., the global market) can strengthen firms’ security awareness. The authors also call for an integrated security management system, e.g., communication strategies for sharing information to mitigate SCS risks, emphasising that a collaborative security system with supply chain partners can help individual firms to better achieve SCS goals.

Voss and Williams (2013), and Lu and Koufteros (2014) studied specific SCS initiatives (e.g., C-TPAT as a third-party SCS management system and Interactional Ship and Port Facility Security Code as shipping security system) and their performance effects on adopting parties. The former study introduced a concept called relational security to account for private-public partnership in security management, and they emphasised the importance and effectiveness of such partnership in maintaining a secure global supply chain. The second study identified five major sources of pressure to adopt security practice, which are the government, customers, peer firms, norms, and performance, based on the institutional theory perspective.

The articles in this main path provide insightful discussion on the effectiveness of various security management systems by highlighting how SCS management standards (e.g., C-TPAT) initiated by the government, professional organisations (e.g., ISO), or leading enterprise (e.g., IBM launched a plethora of SCS standard) benefit adopter firms.

The value of standard SCS management practices shall be delivered to the targeting firms. However, the moderating effects of adoption incentives and other antecedents to adoption have not been adequately discussed. Whether the firm's operational capability affects the effectiveness of SCS management practice and how external contingencies affect the likelihood of SCS practice implementation are important research questions not yet adequately addressed. Security management systems are primarily designed to prevent security accidents. Future research in this cluster can examine the effectiveness of SCS management systems with a more objective approach. For example, researchers can examine the abnormal change of security performance (in terms of security accident rate) or financial performance (in terms of stock return) after adopting security management systems.

Figure 9 The main path for cluster 2 (*security management systems*)



4.4 Cluster 3: transportation security

This cluster discusses security issues in the transportation and shipping industries. Lee and Whang (2005) proposed a model to minimise the cost of achieving security targets and the model is based on quality cost analysis. Similar to the quality manager approach for cost reduction, operations manager can also lower the security cost by properly applying SCS practices. Therefore, they analysed various security initiatives, and compared and contrasted with quality management practices, bringing insights to transportation security from a quality management perspective.

Thibault et al. (2006) reported findings on how logistics and maritime firms respond to the trend of security management. Based on interviews with senior container line executives, port officials, and marine terminal security officers, they highlighted the importance of maritime security for managing international cargo flows. For firms that are actively involved in cross-border logistics security initiatives with feedback provided to the government, their chances of successful security management are much higher.

Considering that both cargo and information flows are critical to container transport chain management, Lun et al. (2008) adopted the institutional theory perspective to analyse various isomorphic pressures in the transportation industry that lead organisations to adopt security management information systems. Security management technologies (e.g., radio-frequency identification (RFID) technology, container non-intrusive inspection (NII) technology, and smart box initiative) were investigated. Their study

sheds light on the effect of each institutional isomorphism, i.e., *coercion*, *mimesis*, and *norms*, on the adoption of container security technology.

Yang (2011) focused on Taiwan's maritime SCS and identified the security factors that may adversely influence container security. Moreover, they suggested considering efficiency, competition, and cost to strike a balance between security improvement and cost reduction.

Williams et al. (2009a) and Yang et al. (2013) enriched safety and security management research on container shipping by conducting a case study and a survey research. The former employs a combination of qualitative and quantitative methods to identify and rank the risk factors. The latter provides a comprehensive study of the impact of security management on the performance of container shipping operations.

The articles in the main path of this cluster relate to a specific industry (i.e., transportation). Since security breaches frequently occur in shipping and transport operations (e.g., theft of cargo), this stream of research not only introduces the methodologies (e.g., case study/survey) that can be applied to understand how to enhance the level of security in transportation, but also offers managerial implications on how SCS issues are managed in shipping and transport operations. However, the above studies have an insufficient emphasis on the unique characteristics of the transportation industry, such as the location and connectivity of a seaport. The current literature only investigates how popular security programs have been generically applied in the transportation industry. It is noteworthy that maritime transportation has been playing the most active role in global cargo movement in terms of container/dry bulk/tanker volumes. Accordingly, we should pay extra attention to security issues in the maritime transportation industry. Research questions such as:

- 1 how to help long-distance cargo movement to achieve fewer service variations and security breaches during transit and storage
- 2 how to incorporate security concerns into maritime transport system design (e.g., port and route planning) at the early stage, should be investigated in future study.

Placing security issues as a priority at the system designing stage could reduce the cost of system reconfiguration when a security breach occurs.

4.5 Cluster 4: terrorism

This cluster contains six articles. The traversal weights for the articles in this cluster are highly similar, implying that all the articles are equally important. Unlike the other clusters, no main path knowledge structure can be established. Considering the small sample size in this cluster, we consider terrorism research with an OM focus should be further developed.

This cluster covers the public policy of preventing terrorist attacks. The optimal solutions of cost saving, efficiency enhancement, and prevention of terrorism disruption are discussed. For example, Pinker (2007) developed mathematical models for assessing a defensive mechanism comprising private and public warnings of security breaches. Other studies seek to resolve the conflicts that governments' anti-terrorism departments often encountered. Governments' anti-terrorism related departments need to ensure adequate inspections of suspicious cargoes at the customs, while simultaneously minimising the congestion caused by intensive inspections (Bakshi and Gans, 2010).

Given the growing terrorism concerns, we suggest the following directions to mitigate such threats in future research.

- 1 Examine the effectiveness of security regulations across countries and how they affect the trading activities globally.
- 2 Investigate where the blind spots of the global logistics for terroristic activities are.
- 3 how to balance the level of security and efficiency in international trade.

Research works in the above clusters not only contribute to specific security concerns in supply chain management, but also provide additional insights into the supply chain risk literature. Especially for cluster 3 – transportation security and cluster 4 – terrorism, which is perceived as the primary and growing risks in the global supply chain in recent years, should receive greater attention from the academia to assess their potential impacts on firms' overall risk. How the studies in cluster 2 – security management system could help effectively reduce the risks discussed in clusters 3 and 4 would be an important research avenue for future research.

5 Future research directions and limitation of the methodology

First, we call for more research on security management in the downstream supply chain which deals SCS problems with customers. It is because service defection (e.g., providers cannot deliver service on time due to SCS breaches) caused by security accidents can lead to severe adverse consequences for manufacturers or transport carriers, eventually harming the entire supply chain. For instance, a previous study has investigated how an individual's regulatory focus, level of risk, and uncertainty of supply chain disruption affect supply chain employees' strategy to mitigate disruption (Cantor et al., 2014). This study can be extended to investigate how employees (e.g., operations or security managers) in manufacturing firms or transport firms assess the security risk levels from their suppliers and establish effective strategies to mitigate such security risk. In addition, the methodologies used in empirical studies are limited to case study and survey, either of which is subject to criticisms (e.g., sample selection bias, reliability of respondents, etc). To overcome this methodological deficiency, future research should consider using objective data to measure firm performance outcomes after the adoption of SCS practices or after a security breach.

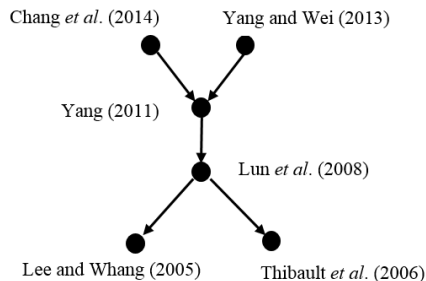
Second, in the matrix for CNA, the algorithm does not distinguish the importance of each citation to a sample article. However, in reality, some references are cited only for simple utility and used for a small part of the paper while others may contribute to the major foundation of the research. We acknowledge that the CNA approach to clustering fails to take this distinction into consideration. We can weigh the importance of each citation based on the application of each corresponding cited article in each sample article to strengthen the robustness of CNA.

Finally, as CNA is dependent on citation numbers and neutrality between citations, it may include 'inappropriate citation', e.g., a citation used as a counter-example to provide evidence on the inappropriateness of the cited paper. The limitation of this study is that we cannot confirm the relationship between the citing paper and the cited paper. Future studies could identify the inappropriate citations to mitigate possible sample selection errors.

6 New theoretical framework for SCS management

The above review outlines the extant knowledge structure of SCS studies, which can help academia and practitioners identify research opportunities to extend this research stream. However, there is a lack of systematic framework to explain security management issues in practice or theorise the antecedents for adoption, the mechanisms for managing implementation, and performance outcomes of SCS practices adoption. A lack of knowledge development hinders the ability of scholars to explain why firms adopt (or not to adopt) SCS practices and how they perform in the implementation outcomes. We propose a framework to facilitate knowledge development of SCS management by integrating the above-discussed issues (see Figure 10).

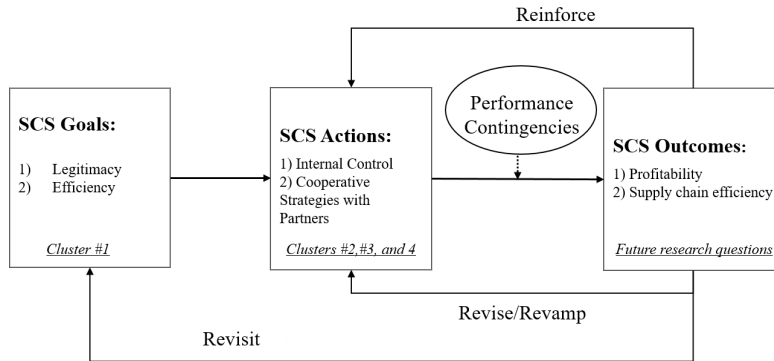
Figure 10 The main path for cluster 3 (*transportation security*)



We suggest a model to account for the influence of external environment on firm's decision making (Lun et al., 2008) based on the organisational performance feedback theoretical perspective (Greve, 1998). Successful implementation of SCS practices needs to follow three steps: setting SCS goals, taking actions to implement, and reinforcing the practices (if the feedback is good) or refining the practices (if the feedback is not good) and adjusting the goals to a proper extent. Usually firms set their SCS goals to achieve legitimacy (e.g., follow the industry norms to adopt a security management certification) or improve operational efficiency by security management. For SCM, firms take various actions to strengthen their SCS and the related practices can be broadly categorised as internal control (e.g., employee security training and regular inspections) and cooperative strategies with partners (e.g., joint site inspections with the US Customs and Border Protection). Finally, firms need to assess the performance of these practices and take improvement actions where appropriate. Contingency theory suggests that the performance outcome of an organisational practice is contingent upon firm's internal and external environments (Grötsch et al., 2013). Therefore, firms operating under different environments ('performance contingencies' in Figure 10) may attain different security performance outcomes. Firms can repeat the established security routines to continuously address security problems if the current performance outcomes are considered satisfactory. In contrast, when their security goals set are not met, they may revisit the goals with proper adjustments and revamp the practices. This research framework pinpoints possible determinants of SCS practices adoption, the performance contingency, and the performance feedback mechanism (reinforce, revise, and revamp), facilitating

future studies to extend this stream of research, for example, the training and development requirements for SCS (Hwang et al., 2017) and the critical success factors of SCS influencing logistics performance (Aserkar et al., 2017).

Figure 11 Research framework for SCS management



Notes: Cluster #1: SCS conceptualisation and application; cluster #2: security management system; cluster #3: transportation security; cluster #4: terrorism. Cluster #1 helps managers properly set their SCS goals while the insights in cluster #2, #3, and #4 are good for managers to take references when implementing SCS practices. As mentioned in Section 5, the future research may use objective (archive) data to measure SCS performance outcome which would overcome the basis caused by perceptual constructs in previous survey studies.

7 Conclusions

We review 143 sample research studies on SCS management, from which we identify four major research domains by CNA, which provides an objective approach for clustering research topics. Moreover, we apply MPA to outline the development of the knowledge structure in each research domain and suggest future research avenues in each research domain under the SCS theme. This paper contributes to the literature on SCS research with an OM/OR focus on the following aspects. We identify and analyse the research domains under SCS, and show the main path of studies within each domain. These findings help researchers identify fundamental studies in each research domain and enable them to position their studies in an appropriate research domain and research gaps. Moreover, we identify research gaps on the main path and suggest potential research directions for SCS management.

References

- Aserkar, R., Kumthekar, N. and Inamdar, S. (2017) 'Training and development needs of logistics and supply chain professionals in South Asia', *International Journal of Shipping and Transport Logistics*, Vol. 9, No. 1, pp.85–106.
- Autry, C.W. and Bobbitt, M.L. (2008) 'Supply chain security orientation: conceptual development and a proposed framework', *The International Journal of Logistics Management*, Vol. 19, No. 1, pp.42–64.
- Bakshi, N. and Gans, N. (2010) 'Securing the containerized supply chain: analysis of government incentives for private investment', *Management Science*, Vol. 56, No. 2, pp.219–233.
- Bakshi, N. and Kleindorfer, P. (2009) 'Co-opetition and investment for supply-chain resilience', *Production and Operations Management*, Vol. 18, No. 6, pp.583–603.
- Bearzotti, L.A., Salomone, E. and Chiotti, O.J. (2012) 'An autonomous multi-agent approach to supply chain event management', *International Journal of Production Economics*, Vol. 135, No. 1, pp.468–478.
- Berle, Ø., Rice Jr., J.B. and Asbjørnslett, B.E. (2011) 'Failure modes in the maritime transportation system: a functional approach to throughput vulnerability', *Maritime Policy & Management*, Vol. 38, No. 6, pp.605–632.
- Braunscheidel, M.J. and Suresh, N.C. (2009) 'The organizational antecedents of a firm's supply chain agility for risk mitigation and response', *Journal of Operations Management*, Vol. 27, No. 2, pp.119–140.
- Cantor, D.E., Blackhurst, J.V. and Cortes, J.D. (2014) 'The clock is ticking: the role of uncertainty, regulatory focus, and level of risk on supply chain disruption decision making behavior', *Transportation Research Part E: Logistics and Transportation Review*, December, Vol. 72, pp.159–172.
- Chang, C-H., Xu, J. and Song, D-P. (2014) 'An analysis of safety and security risks in container shipping operations: a case study of Taiwan', *Safety Science*, March, Vol. 63, pp.168–178.
- Chopra, S. and Sodhi, M.S. (2004) 'Managing risk to avoid supply-chain breakdown', *MIT Sloan Management Review*, Vol. 46, No. 1, p.53.
- Christopher, M., Mena, C., Khan, O. and Yurt, O. (2011) 'Approaches to managing global sourcing risk', *Supply Chain Management: An International Journal*, Vol. 16, No. 2, pp.67–81.
- Clauset, A., Newman, M.E. and Moore, C. (2004) 'Finding community structure in very large networks', *Physical Review E*, Vol. 70, No. 6, p.066111.
- Closs, D.J. (2008) 'A framework for protecting your supply chain', *Supply Chain Management Review*, Vol. 12, No. 2, pp.38–45.
- Colicchia, C. and Strozzi, F. (2012) 'Supply chain risk management: a new methodology for a systematic literature review', *Supply Chain Management: An International Journal*, Vol. 17, No. 4, pp.403–418.
- De Meo, P., Ferrara, E., Fiumara, G. and Provetti, A. (2011) 'Generalized Louvain method for community detection in large networks', *Intelligent Systems Design and Applications (ISDA), 2011 11th International Conference*, IEEE, pp.88–93.
- De Nooy, W., Mrvar, A. and Batagelj, V. (2005) *Exploratory Social Network Analysis with Pajek*, Cambridge University Press, New York.
- Dobie, K. (2005) 'The core shipper concept: a proactive strategy for motor freight carriers', *Transportation Journal*, Vol. 44, No. 2, pp.37–53.
- Fahimnia, B., Sarkis, J. and Davarzani, H. (2015) 'Green supply chain management: a review and bibliometric analysis', *International Journal of Production Economics*, April, Vol. 162, pp.101–114.

- Fan, D., Lo, C.K., Ching, V. and Kan, C. (2014) 'Occupational health and safety issues in operations management: a systematic and citation network analysis review', *International Journal of Production Economics*, December, Vol. 158, pp.334–344.
- Fang, J., Zhao, L., Fransoo, J.C. and Van Woensel, T. (2013) 'Sourcing strategies in supply risk management: an approximate dynamic programming approach', *Computers & Operations Research*, Vol. 40, No. 5, pp.1371–1382.
- Feng, Y., Zhu, Q. and Lai, K.H. (2017) 'Corporate social responsibility for supply chain management: a literature review and bibliometric analysis', *Journal of Cleaner Production*, August, Vol. 158, pp.296–307.
- Girvan, M. and Newman, M.E. (2002) 'Community structure in social and biological networks', *Proceedings of the National Academy of Sciences*, Vol. 99, No. 12, pp.7821–7826.
- Godfrey, P.C., Merrill, C.B. and Hansen, J.M. (2009) 'The relationship between corporate social responsibility and shareholder value: an empirical test of the risk management hypothesis', *Strategic Management Journal*, Vol. 30, No. 4, pp.425–445.
- Greve, H.R. (1998) 'Performance, aspirations, and risky organizational change', *Administrative Science Quarterly*, Vol. 42, No. 1, pp.58–86.
- Grötsch, V.M., Blome, C. and Schleper, M.C. (2013) 'Antecedents of proactive supply chain risk management – a contingency theory perspective', *International Journal of Production Research*, Vol. 51, No. 10, pp.2842–2867.
- Hameri, A-P. and Hintsa, J. (2009) 'Assessing the drivers of change for cross-border supply chains', *International Journal of Physical Distribution & Logistics Management*, Vol. 39, No. 9, pp.741–761.
- Hwang, D.W., Hong, P.C. and Lee, D.Y. (2017) 'Critical factors that affect logistics performance: a comparison of China, Japan and Korea', *International Journal of Shipping and Transport Logistics*, Vol. 9, No. 1, pp.107–129.
- Jamali, D. and Neville, B. (2011) 'Convergence versus divergence of CSR in developing countries: an embedded multi-layered institutional lens', *Journal of Business Ethics*, Vol. 102, No. 4, pp.599–621.
- Jüttner, U., Peck, H. and Christopher, M. (2003) 'Supply chain risk management: outlining an agenda for future research', *International Journal of Logistics: Research and Applications*, Vol. 6, No. 4, pp.197–210.
- Kleindorfer, P.R. and Saad, G.H. (2005) 'Managing disruption risks in supply chains', *Production and Operations Management*, Vol. 14, No. 1, pp.53–68.
- Knemeyer, A.M., Zinn, W. and Eroglu, C. (2009) 'Proactive planning for catastrophic events in supply chains', *Journal of Operations Management*, Vol. 27, No. 2, pp.141–153.
- Kouvelis, P., Chambers, C. and Wang, H. (2006) 'Supply chain management research and production and operations management: review, trends, and opportunities', *Production and Operations Management*, Vol. 15, No. 3, pp.449–469.
- Kumar, S. and Verruso, J. (2008) 'Risk assessment for the security of inbound containers at US ports: a failure, mode, effects, and criticality analysis approach', *Transportation Journal*, Vol. 47, No. 4, pp.26–41.
- Kumar, S., Jensen, H. and Menge, H. (2008) 'Analyzing mitigation of container security risks using six sigma DMAIC approach in supply chain design', *Transportation Journal*, Vol. 47, No. 2, pp.54–66.
- Laequuddin, M., Sardana, G., Sahay, B., Abdul Waheed, K. and Sahay, V. (2009) 'Supply chain partners' trust building process through risk evaluation: the perspectives of UAE packaged food industry', *Supply Chain Management: An International Journal*, Vol. 14, No. 4, pp.280–290.
- Lee, D-H., Song, L. and Wang, H.Q. (2008) 'An optimization approach to security operations toward sustainable seaport', *International Journal of Sustainable Transportation*, Vol. 2, No. 2, pp.115–133.

- Lee, H.L. and Whang, S. (2005) 'Higher supply chain security with lower cost: lessons from total quality management', *International Journal of Production Economics*, Vol. 96, No. 3, pp.289–300.
- Lee, J., Palekar, U.S. and Qualls, W. (2011) 'Supply chain efficiency and security: coordination for collaborative investment in technology', *European Journal of Operational Research*, Vol. 210, No. 3, pp.568–578.
- Lewis, M.A. (2003) 'Cause, consequence and control: towards a theoretical and practical model of operational risk', *Journal of Operations Management*, Vol. 21, No. 2, pp.205–224.
- Lockamy Iii, A. and McCormack, K. (2010) 'Analysing risks in supply networks to facilitate outsourcing decisions', *International Journal of Production Research*, Vol. 48, No. 2, pp.593–611.
- Lodree Jr., E.J. and Taskin, S. (2008) 'An insurance risk management framework for disaster relief and supply chain disruption inventory planning', *Journal of the Operational Research Society*, Vol. 59, No. 5, pp.674–684.
- Lu, G. and Koufteros, X.A. (2014) 'Adopting security practices for transport logistics: institutional effects and performance drivers', *International Journal of Shipping and Transport Logistics*, Vol. 6, No. 6, pp.611–631.
- Lu, G., Koufteros, X. and Lucianetti, L. (2017) 'Supply chain security: a classification of practices and an empirical study of differential effects and complementarity', *IEEE Transactions on Engineering Management*, Vol. 64, No. 2, pp.234–248.
- Lun, Y.V., Wong, C.W., Lai, K.H. and Cheng, T. (2008) 'Institutional perspective on the adoption of technology for the security enhancement of container transport', *Transport Reviews*, Vol. 28, No. 1, pp.21–33.
- Männistö, T., Hintsala, J. and Urciuoli, L. (2014) 'Supply chain crime – taxonomy development and empirical validation', *International Journal of Shipping and Transport Logistics*, Vol. 6, No. 3, pp.238–256.
- Manuj, I. and Mentzer, J.T. (2008) 'Global supply chain risk management strategies', *International Journal of Physical Distribution & Logistics Management*, Vol. 38, No. 3, pp.192–223.
- Marley, K.A., Ward, P.T. and Hill, J.A. (2014) 'Mitigating supply chain disruptions – a normal accident perspective', *Supply Chain Management: An International Journal*, Vol. 19, No. 2, pp.142–152.
- Marlow, P.B. (2010) 'Maritime security: an update of key issues', *Maritime Policy & Management*, Vol. 37, No. 7, pp.667–676.
- Marucheck, A., Greis, N., Mena, C. and Cai, L. (2011) 'Product safety and security in the global supply chain: issues, challenges and research opportunities', *Journal of Operations Management*, Vol. 29, No. 7, pp.707–720.
- Marufuzzaman, M., Eksioğlu, S.D. and Huang, Y.E. (2014) 'Two-stage stochastic programming supply chain model for biodiesel production via wastewater treatment', *Computers & Operations Research*, September, Vol. 49, pp.1–17.
- Meixell, M.J. and Gargeya, V.B. (2005) 'Global supply chain design: a literature review and critique', *Transportation Research Part E: Logistics and Transportation Review*, Vol. 41, No. 6, pp.531–550.
- Meixell, M.J. and Norbis, M. (2012) 'Integrating carrier selection with supplier selection decisions to improve supply chain security', *International Transactions in Operational Research*, Vol. 19, No. 5, pp.711–732.
- Melnik, S.A., Ritchie, W.J. and Calantone, R.J. (2013) 'The case of the C-TPAT border security initiative: assessing the adoption/persistence decisions when dealing with a novel, institutionally driven administrative innovation', *Journal of Business Logistics*, Vol. 34, No. 4, pp.289–300.
- Mueller, J. and Stewart, M.G. (2012) 'The terrorism delusion: America's overwrought response to September 11', *International Security*, Vol. 37, No. 1, pp.81–110.

- Neiger, D., Rotaru, K. and Churilov, L. (2009) 'Supply chain risk identification with value-focused process engineering', *Journal of Operations Management*, Vol. 27, No. 2, pp.154–168.
- Papadakis, I.S. (2006) 'Financial performance of supply chains after disruptions: an event study', *Supply Chain Management: An International Journal*, Vol. 11, No. 1, pp.25–33.
- Pero, M. and Sudy, I. (2014) 'Increasing security and efficiency in supply chains: a five-step approach', *International Journal of Shipping and Transport Logistics*, Vol. 6, No. 3, pp.257–279.
- Pilkington, A. and Meredith, J. (2009) 'The evolution of the intellectual structure of operations management – 1980–2006: a citation/co-citation analysis', *Journal of Operations Management*, Vol. 27, No. 3, pp.185–202.
- Pinker, E.J. (2007) 'An analysis of short-term responses to threats of terrorism', *Management Science*, Vol. 53, No. 6, pp.865–880.
- Prokop, D. (2012) 'Smart containers and the public goods approach to supply chain security', *International Journal of Shipping and Transport Logistics*, Vol. 4, No. 2, pp.124–136.
- Radicchi, F., Castellano, C., Cecconi, F., Loreto, V. and Parisi, D. (2004) 'Defining and identifying communities in networks', *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 101, No. 9, pp.2658–2663.
- Revilla, E. and Sáenz, M.J. (2014) 'Supply chain disruption management: Global convergence vs. national specificity', *Journal of Business Research*, Vol. 67, No. 6, pp.1123–1135.
- Roth, A.V., Tsay, A.A., Pullman, M.E. and Gray, J.V. (2008) 'Unraveling the food supply chain: strategic insights from China and the 2007 recalls', *Journal of Supply Chain Management*, Vol. 44, No. 1, pp.22–39.
- Russell, D.M. and Saldanha, J.P. (2003) 'Five tenets of security-aware logistics and supply chain operation', *Transportation Journal*, Vol. 42, No. 4, pp.44–54.
- Sarathy, R. (2006) 'Security and the global supply chain', *Transportation Journal*, Vol. 45, No. 4, pp.28–51.
- Sheffi, Y. and Rice Jr., J.B. (2005) 'A supply chain view of the resilient enterprise', *MIT Sloan Management Review*, Vol. 47, No. 1, p.41.
- Sheu, C., Lee, L. and Niehoff, B. (2006) 'A voluntary logistics security program and international supply chain partnership', *Supply Chain Management: An International Journal*, Vol. 11, No. 4, pp.363–374.
- Sheu, J.-B. (2007) 'An emergency logistics distribution approach for quick response to urgent relief demand in disasters', *Transportation Research Part E: Logistics and Transportation Review*, Vol. 43, No. 6, pp.687–709.
- Skipper, J.B. and Hanna, J.B. (2009) 'Minimizing supply chain disruption risk through enhanced flexibility', *International Journal of Physical Distribution & Logistics Management*, Vol. 39, No. 5, pp.404–427.
- Smith, G., Watson, K., Baker, W. and Pokorski II, J. (2007) 'A critical balance: collaboration and security in the IT-enabled supply chain', *International Journal of Production Research*, Vol. 45, No. 11, pp.2595–2613.
- 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*, Vol. 29, No. 7, pp.721–736.
- Stewart, G.T., Kolluru, R. and Smith, M. (2009) 'Leveraging public-private partnerships to improve community resilience in times of disaster', *International Journal of Physical Distribution & Logistics Management*, Vol. 39, No. 5, pp.343–364.
- Thai, V.V. (2009) 'Effective maritime security: conceptual model and empirical evidence', *Maritime Policy & Management*, Vol. 36, No. 2, pp.147–163.
- Thibault, M., Brooks, M.R. and Button, K.J. (2006) 'The response of the US maritime industry to the new container security initiatives', *Transportation Journal*, Vol. 45, No. 1, pp.5–15.

- Tomlin, B. (2006) 'On the value of mitigation and contingency strategies for managing supply chain disruption risks', *Management Science*, Vol. 52, No. 5, pp.639–657.
- Trkman, P. and McCormack, K. (2009) 'Supply chain risk in turbulent environments – a conceptual model for managing supply chain network risk', *International Journal of Production Economics*, Vol. 119, No. 2, pp.247–258.
- Voss, M.D. and Williams, Z. (2013) 'Public-private partnerships and supply chain security: C-TPAT as an indicator of relational security', *Journal of Business Logistics*, Vol. 34, No. 4, pp.320–334.
- Voss, M.D., Closs, D.J., Calantone, R.J., Helfferich, O.K. and Speier, C. (2009a) 'The role of security in the food supplier selection decision', *Journal of Business Logistics*, Vol. 30, No. 1, pp.127–155.
- Voss, M.D., Whipple, J.M. and Closs, D.J. (2009b) 'The role of strategic security: internal and external security measures with security performance implications', *Transportation Journal*, Vol. 48, No. 2, pp.5–23.
- Wakolbinger, T. and Cruz, J. (2011) 'Supply chain disruption risk management through strategic information acquisition and sharing and risk-sharing contracts', *International Journal of Production Research*, Vol. 49, No. 13, pp.4063–4084.
- Wang, X. and Zhuang, J. (2011) 'Balancing congestion and security in the presence of strategic applicants with private information', *European Journal of Operational Research*, Vol. 212, No. 1, pp.100–111.
- Whipple, J.M., Voss, M.D. and Closs, D.J. (2009) 'Supply chain security practices in the food industry: do firms operating globally and domestically differ?', *International Journal of Physical Distribution & Logistics Management*, Vol. 39, No. 7, pp.574–594.
- Williams, Z., Lueg, J.E. and Lemay, S.A. (2008) 'Supply chain security: an overview and research agenda', *The International Journal of Logistics Management*, Vol. 19, No. 2, pp.254–281.
- Williams, Z., Lueg, J.E., Taylor, R.D. and Cook, R.L. (2009a) 'Why all the changes? An institutional theory approach to exploring the drivers of supply chain security (SCS)', *International Journal of Physical Distribution & Logistics Management*, Vol. 39, No. 7, pp.595–618.
- Williams, Z., Ponder, N. and Autry, C.W. (2009b) 'Supply chain security culture: measure development and validation', *The International Journal of Logistics Management*, Vol. 20, No. 2, pp.243–260.
- Wilson, M.C. (2007) 'The impact of transportation disruptions on supply chain performance', *Transportation Research Part E: Logistics and Transportation Review*, Vol. 43, No. 4, pp.295–320.
- Wu, T., Blackhurst, J. and O'grady, P. (2007) 'Methodology for supply chain disruption analysis', *International Journal of Production Research*, Vol. 45, No. 7, pp.1665–1682.
- Yang, C-C. and Wei, H-H. (2013) 'The effect of supply chain security management on security performance in container shipping operations', *Supply Chain Management: An International Journal*, Vol. 18, No. 1, pp.74–85.
- Yang, Y-C. (2010) 'Impact of the container security initiative on Taiwan's shipping industry', *Maritime Policy & Management*, Vol. 37, No. 7, pp.699–722.
- Yang, Y-C. (2011) 'Risk management of Taiwan's maritime supply chain security', *Safety Science*, Vol. 49, No. 3, pp.382–393.
- Yang, Z., Ng, A.K. and Wang, J. (2013) 'Prioritising security vulnerabilities in ports', *International Journal of Shipping and Transport Logistics*, Vol. 5, No. 6, pp.622–636.
- Yip, T.L. (2008) 'Port traffic risks – a study of accidents in Hong Kong waters', *Transportation Research Part E: Logistics and Transportation Review*, Vol. 44, No. 5, pp.921–931.
- Zhu, X. (2016) 'Managing the risks of outsourcing: time, quality and correlated costs', *Transportation Research Part E: Logistics and Transportation Review*, October, Vol. 90, pp.121–133.

Zhuang, J., Bier, V.M. and Alagoz, O. (2010) 'Modeling secrecy and deception in a multiple-period attacker-defender signaling game', *European Journal of Operational Research*, Vol. 203, No. 2, pp.409–418.

Notes

- 1 Because more recently published papers are less likely cited by other papers, the likelihood of being clustered into a research group of these papers tends to be very low. We set 2015 as the ending year to enhance the effectiveness of citation network analysis.
- 2 There are indeed various software for conducting citation network analysis. However, it is considered that no distinct difference exist among these software because the algorithms cited by them are more or less the same. In addition, *HistCite* and *Gephi* have been widely adopted in previous studies for citation network analysis (e.g., Fahimnia et al., 2015; Fan et al., 2014).
- 3 The deduction of sample papers is also acknowledged by recently published articles using the citation network analysis (see Fan et al., 2014; Feng et al., 2017).

Appendix

Table A1 Research articles in each research domain

<i>Research focus/domain</i>	<i>Papers</i>
1 SCS conceptualisation and application	Bakshi and Kleindorfer (2009); Bearzotti et al. (2012); Braunscheidel and Suresh (2009); Chopra and Sodhi (2004); Christopher et al. (2011); Colicchia and Strozzi (2012); Kleindorfer and Saad (2005); Knemeyer et al. (2009); Kouvelis et al. (2006); Laeequddin et al. (2009); Lockamy and McCormack (2010); Lodree and Taskin (2008); Marley et al. (2014); Neiger et al. (2009); Papadakis (2006); Revilla and Sáenz (2014); Sheffi and Rice (2005); Skipper and Hanna (2009); Smith et al. (2007); Stewart et al. (2009); Tomlin (2006); Trkman and McCormack (2009); Wakolbinger and Cruz (2011); Whipple et al. (2009); Wilson (2007); Wu et al. (2007)
2 Security management systems	Autry and Bobbitt (2008); Dobie (2005); Hameri and Hints (2009); Kumar et al. (2008); Lu and Koufteros (2014); Maruchek et al. (2011); Meixell and Norbis (2012); Pero and Sudy (2014); Prokop (2012); Roth et al. (2008); Russell and Saldanha (2003); Sheu et al. (2006); Speier et al. (2011); Voss et al. (2009b); Voss and Williams (2013); Whipple et al. (2009); Williams et al. (2008, 2009a, 2009b)
3 Transportation security	Berle et al. (2011); Chang et al. (2014); Kumar and Verruso (2008); Lee et al. (2008); Lee and Whang (2005); Lee et al. (2011); Lun et al. (2008); Marlow (2010); Sarathy (2006); Thai (2009); Thibault et al. (2006); Voss et al. (2009a); Yang and Wei (2013); Yang (2010, 2011)
4 Terrorism	Bakshi and Gans (2010); Männistö et al. (2014); Manuj and Mentzer (2008); Pinker (2007); Wang and Zhuang (2011); Zhuang et al. (2010)