Towards Digital Supply Chain Risk Surveillance

Edward Kosasih* Alexandra Brintrup*

**Institute for Manufacturing, Department of Engineering, University of Cambridge, CB3 0FS UK (Tel: +44 1223 764615; e-mail: ab702@cam.ac.uk).*

Abstract: In this paper, we define and conceptualize the emerging practice of *"Digital Supply Chain Surveillance* (DSCS)" as the proactive monitoring of digital data that allows firms to track, manage, and analyze information related to a supply chain network without needing the explicit consent of firms involved in the supply chain. After reviewing approaches to surveillance challenges that have been raised, we find that several approaches have been proposed, in particular for risk management, which have made use of Artificial Intelligence (AI) as a key enabler. By interconnecting surveillance data sources and systems, appropriate AI techniques can make surveillance easier, larger scale and possibly more informative, whilst at the same time bringing about a number of technical, ethical and managerial challenges with it. We discuss these challenges, highlighting the need to integrate multiple surveillance data and insights, the potential for hidden bias and the consequent need for AI skills to prevent bias, and the need to design guidance for embedding DSCS insights into business processes ethically, and transparently.

Keywords: Artificial Intelligence, Machine Learning, Supply Chain Risk, Risk Surveillance, Digitalisation

1. INTRODUCTION

Due to their partly designed, partly emergent nature, supply chains suffer from chronic information challenges resulting in unknown supply chain risks, the consequences of which have been well reported in literature (see Ho et al 2015 for a review). Effective supply chain risk management (SCRM) aims to develop methods to prepare for and mitigate risk in supply chains. However, the challenge of identifying and monitoring risk is still a relatively understudied area, causing significant concern to industry. Examples include incidents where companies, unaware of their interdependencies, discover unlawful or ethically questionable practices, counterfeit, dangerous or controversial components and ingredients enter into material flow, and disruptions that ripple through the chain and create disturbances such as stock outs (Ivanov et al. 2018). Typical approaches to identify such risks include customer surveys, accreditation approaches, manual mapping and monitoring of suppliers, third party services. Such approaches tend to be costly, and require significant effort and time investment.

Supply Chain Digitalisation might offer companies a set of additional approaches to complement extant methods to address the problem by enabling a bottom up process, where companies attempt to capture and analyse digital data that could inform them of previously unknown information, without the need to explicitly convince other supply chain actors for sharing it. We assert that the increased appetite for digitalisation in Supply Chains brings about a unique opportunity to remedy, albeit only partially, some of the risk identification and supply chain monitoring challenges observed in SCRM.

Examples would include a buyer checking whether one of their suppliers is supplying to a competitor, an insurance underwriter keeping a close eye on the financial health of a company's supply chain dependencies, or a supplier trying to learn about high value contracts awarded to its buyer so as to increase its bargaining position. Whilst such "*surveillance*" may have already been prevalent in supply chains, it was hitherto pursued manually. The increased use of digital technology makes it possible to automate data capture and analysis at a much larger scale, allowing surveillance to take place quasi real-time, with data obtained from multiple sources. Additionally, digitalisation facilitates a step change in surveillance by interconnecting multiple data sources and systems. Hence surveillance becomes easier, larger scale and possibly more informative. Whilst the use of AI is not a prerequisite to analyse digital data, the vast majority of methods we review in this paper use some form of AI technology, as it provides performance improvements over other methods in dealing with unstructured, large-scale digital data automatically.

In this paper we define the newly emerging field of Digital Supply Chain Surveillance (DSCS), and discuss the role of Artificial Intelligence (AI) in it. We categorise the types of surveillance activities that can be pursued with extant technology, and demonstrate how various sources of information can be brought together. We then highlight some of the challenges and pitfalls that need to be researched within this area.

2. DIGITAL SUPPLY CHAIN SURVEILLANCE

2.1. Definitions

Surveillance refers to "*close watch kept over someone (Merriam-Webster dictionary)*" or "*the focused, systematic, and routine attention to personal details for purposes of influence, management, protection, or direction*"

whereas the term "*Digital Surveillance*" has negative, or controversial connotations, because the term is taken to mean: "*the acquisition and consolidation of very large volumes of personal data, and its exploitation by commercial enterprises to target advertisements, manipulate consumer behaviour*" *(Clarke 2019)*". A key feature of surveillance systems is to identify, localise and diagnose source of problems (Shinde, 2012). Researchers agree that digitalisation of surveillance is significant because of the ubiquity of data, and the speed with which it is generated, which enables the algorithmic facilitation of detection, tracking, sorting, prediction in an automated manner (*Clarke 2019*).

Within the supply chain management context, it is not individuals, but rather organisations and products that are monitored. We define *Digital Supply Chain Surveillance (DSCS)* as the proactive monitoring of digital data that allows firms to track, manage and analyse information related to a supply chain network without the explicit consent of firms involved in the supply chain. DSCS involves three key phases: i) data collection and processing, ii) data analysis, iii) extraction of actionable insight. The first phase would involve the selection of appropriate data sources, devising methods and algorithms to collect and process data. The second phase necessitates the application of algorithms that derive relevant statistical patterns underlying the dataset. The third phase is about extracting applicable, relevant messages that can help with improved decision making regarding the surveillance challenge. While AI is not an explicit prerequisite for DSCS, all three phases benefit from AI's ability to acquire and process large volumes of digital data in an automated manner. Thus we assert that two key enablers of DSCS are the availability of digitalised Supply Chain data and AI.

Digitalised data sources may include datasets that are internally, or publicly available to organisations, or are available on subscription. DSCS would consist of using such data to extract insights that was previously non-obvious for the surveillance challenge that is being addressed. For instance, ERP data is typically used to plan and monitor transactions relating to supplier orders. Recent studies show that this type of data can be used to predict supplier delays or even possible relations between suppliers (Brintrup et al. 2018). Data that is externally available may consist of social media, company annual reports, and news outlets and others, that may then be used to infer disruptions, supplier-buyer relations, financial health, and production capabilities.

In recent years, an increasing number of studies have proposed ways that exploit digital data to address a number of DSCS challenges, but these studies remain disconnected from one another. We posit that framing these trends within the realm of DSCS will help link extant work and help determine future research directions that need to be tackled.

Within this contextualisation, we direct the attention of the reader to a number of key questions. First of these is: "*What are the surveillance requirements of companies that DSCS can address*?" Secondly, "Which stakeholders are interested in different surveillance challenges?", thirdly "*How can AI facilitate DSCS requirements?*", and finally, "*What are the challenges involved in the application of DSCS?*". We review these next.

2. 2. Surveillance challenges and digital solution approaches

Table 1 shows various supply chain surveillance challenges that have been identified following extant supply chain risk categorisations from literature (see Ho et al. 2015 for a review) and exemplified what the challenge may entail. In addition to surveillance challenges, five types of surveillance stakeholders were identified: Buyer, Supplier, Financer, Insurer, and Regulatory bodies. *Buyers* are organisations that purchase the goods or services of a supplier, whereas *Suppliers* are those who sell them. *Financers* are providers of funds and capital to support buyers and suppliers, and may include banks, supply chain financing organisations and other lenders. *Insurers* are organisations that underwrite supply chain risk. *Regulatory bodies* are government authorities that regulate compliance requirements such as anti-slavery, health and safety laws, and environmentally responsible conduct. For each of the challenges identified, approaches that have been proposed to tackle a given DSCS challenge have been included.

Challenge A, B and C relate to the *supply and quality risks*. With large-scale outsourcing of manufacturing to suppliers, delays in delivery and the management of quality become key issues. While supplier quality prediction remains an understudied area of investigation, a number of DSCS approaches have been proposed to predict supply risk. O'Leary, 2015 proposed the use of Twitter data to monitor supplier disruptions. Baryannis et al., 2019 and Brintrup et al., 2020 created classification algorithms to predict supplier delays using historical delivery data which can then be used to optimise inventory and safety stock. They highlighted explainability to be an important issue to be tackled in the choice of algorithm, and that there may be performance trade offs between explainability and algorithmic performance.

Challenges D, E and F pertain to *network related risk* where risk identification necessitates an element of network discovery. Here the buyer or insurer is interested in a firm's extended connections and risk they are exposed to. Lack of visibility remains a significant challenge for companies. Several studies have shown how lack of visibility can impact supply chain resilience when disruptions ripple through the chain and highlighted the need for improvement (Kinra et al., 2020). For example in D, a buyer would like to know the likelihood of being exposed to suppliers in a certain geolocation, so as to plan for risks such as natural disasters, social or political unrest. Supply chain insurance underwriters would also benefit from knowing how their insurance client may be affected by disruptions. In E, a buyer would like to know whether its supplier is supplying to a competitor firm, which would be relevant in the case of disruptions where the supplier might prioritize another customer. In F, the buyer would like to know whether its suppliers are engaged in a procurement relationship they are unaware of. If this is the case, the buyer might experience multiple disruptions as the highly connected supplier runs into problems, affecting further upstream companies. To address these challenges a small

number of studies have investigated how DSCS can complement supply chain mapping and monitoring efforts. (Wichmann et al., 2018) created a method to extract supply chain maps from the world wide web using natural language processing. (Brintrup et al., 2018) analyzed how partial knowledge of the supply network could be used to infer hidden dependencies between suppliers not known to the buyer. Their method incorporated classifier algorithms trained using topological and production data. Kosasih et al. (2021) created a Graph Neural Network that considers only topological features, reporting improvements over Brintrup et al. (2018). Aziz et al. (2021) created a Knowledge Graph based approach where supplier data is collected and represented in the form of a graph, enabling practitioners to perform complex queries that may yield previously undetected risk.

Challenges G and H are related to *reputation risk*. In this example, the buyer would like to know the ingredients and the composition of the product it procures. Pharmaceuticals and food manufacturing are typical examples where product composition knowledge may be important. As labelling regulations differ across the globe, comprehensive information of food products containing multiple processed ingredients is not always available, resulting in problems such as horse meat in Ikea Swedish meatballs (Falkheimer & Heide, 2015) and nut allergies in sandwiches ('Pret Allergy Death', 2019). Similar issues may be observed in toys where toxic ingredients have been discovered (*China Halts 'toxic' Toy Exports*, 2007). Researchers are increasingly exploring machine learning and network science to study food supply networks, uncovering patterns relating ingredients to final products (Ahn et al., 2011; Astill et al., 2019) and using AI to identify hidden ingredients not listed for the product. Similarly, Challenge H concerns reputation risk arising from supply chain actors that engage in fraudulent behaviour. Combatting fake products is a global issue in manufacturing. In some countries, it is estimated that up to 40% of automotive parts are counterfeit (Dachowicz et al., 2017), which may lead to quality problems in later manufacturing stages. It is imperative that companies have reassurance that the products they procure are genuine. Although several AI techniques have been developed to detect counterfeit products the use of supply chain data in predicting counterfeit products provides further opportunities to combat this challenge. In this vein, (Zage et al., 2013) proposed a method to identify deceptive practices within the e-commerce supply chain by analyzing online transaction data to detect fraudulent vendors artificially building a good reputation through fake online reviews.

Challenge I focuses on *sustainability risk*. The topic of Environmental, Social and Governance (ESG) is gaining traction across all industries, strongly driven by regulatory compliance and reporting requirements. Researchers are looking into automating aspects of the ESG scoring process (Alikhani et al., 2019) through the use of DSCS. For instance, (Kuo et al., 2010) look at the interests and rights of employee (IRE) and the rights of stakeholders (RS), (Azadnia et al., 2015) study product quality conformation and long-term stability, (Chiou et al., 2008) investigates Environmental Management Systems whereas (Klassen & Vereecke, 2012) study the management of social issues such as child labour, health, safety and discrimination.

Challenges J , K and L are concerned with *financial risk*. The buyer is interested in the financial capability of a supplier to adequately source capital to build and deliver its order and the supplier is interested in the buyer's ability to pay on time and in full. Supply chain financing companies and banks are interested in whether supplier sells to reputable buyers before lending capital to the supplier. (Martínez et al., 2019) use publicly available data on suppliers to predict financial default in supply chain financing. (Ye et al., 2015) used asset-liability ratios for Chinese firms to predict likely supply chain disruption based on a firm's financial performance.

Challenges M, N and P are related to *cost reduction and strategic negotiation*. Many supply chain actors negotiate contracts with large lists of suppliers and buyers dispersed globally. While procurement officers will often manually analyze price negotiation opportunities, DSCS may help provide automated ways to find patterns in pricing to make negotiation more efficient. Researchers have been exploring several techniques such as multi-agent systems to model pricing likelihood and optimized agreements between suppliers and buyers (Jiao et al., 2006, Boateng et al. 2017) based on historical data on supplier prices. Other areas worthy of investigation within DSCS could include capacity prediction, pricing anomaly prediction, and price offer prediction.

Challenge O is about *supplier innovation*, which is a significant criteria in industries such as the automotive sector, as they undergo frequent innovative disruptions such as the transition to electric vehicles. Manufacturers would like to work with innovative suppliers as they may better adapt to changing product specifications and requirements. DSCS may help quantify measurements of innovativeness such as AI based patent analytics on suppliers (Aristodemou & Tietze, 2018; Trautrims et al., 2017).

The above, analysis, while non-exhaustive, points to a number of diverse challenges that DSCS has the potential to address through automated data collection and analysis of digital data. Vast majority of methods that have been proposed involve the use of AI technologies, which both enables DSCS to be automated, and at the same time, brings about a number of challenges itself. We discuss these next.

3. DISCUSSION

At the beginning of Section 2, we noted a number of negative connotations regarding the concept of Digital Surveillance specifically in the context of personal data. Several of these apply also to the digital surveillance of supply chains, including ethical challenges related to the use of AI algorithms in DSCS. Traditional supply chain surveillance was a manual, and at times an opportunistic process, informed by expert knowledge and limited data. The process would involve scrutiny, validation and judgements made by a variety of SC professionals. For example, if a supplier's relations with competitors were of interest, the buyer might directly query the supplier or monitor industrial news sources. At other times, surveillance might be tacit. Procurement officers might collate historical data on supplier performance periodically to

assist in future supplier selection. Both of these involve a degree of subjectivity and tacit human knowledge.

In contrast, AI is known to be particularly good in picking up biases from the dataset on which it is trained (Brennen, 2020). Automated algorithms used in DS should not replace existing modes of surveillance but may complement them. They may remove human discretion but introduce further hidden biases from the training data used or from algorithm design. These may be difficult to tease out without relevant AI skill and expertise. (Lianos & Douglas, 2000) discuss that with the rise of Digital Surveillance, "*the work of human operators shifts from direct mediation and discretion to the design, programming, supervision and maintenance of automated or semi-automatic surveillance systems*". Similarly, in DSCS, AI skills for removing bias will be important, especially when applied to financially impactful use cases that could affect supplier selection, production planning and insurance costing.

Use cases that DSCS may facilitate but were not a part of traditional SCM, necessitate further thought into how the obtained information would be incorporated into existing business processes and management practices. For example, the prediction of excess capacity or financial stress at a supplier have typically not been visible to a buyer. It is important to design processes that handle new information with care, leading to appropriately balanced action. (Graham & Wood, 2003) highlight that the "*characteristic of digital surveillance technologies is their extreme flexibility and ambivalence. On the one hand, systems can be designed to socially exclude, based on automated judgements of social or economic worth; on the other hand, the same systems can be programmed to help overcome social barriers and processes of marginalization"*. Similarly in DSSC, prediction of decreasing performance from a supplier could lead to an automatic action where the supplier's contract is terminated, or to an action that triggers root cause analysis and working to develop and improve the supplier. A case in point is a supplier delivery performance prediction study conducted by an aerospace company (Brintrup et al., 2020), which found that the main cause for delays was the buyer ordering late rather than a performance issue on the side of the supplier. Whilst much care may be given to validate the data and training process, as well as algorithmic design, it is still possible for invalid conclusions or inappropriate actions to emerge from DSCS.

Linked with questions of ethicality in decision making is the question of explainability of AI. Many state of the art AI algorithms are essentially 'black box' methods, which means that interpreting why a certain prediction was made may be difficult. While explainability of AI may refer to various properties (Brennen, 2020), a key one in SCM is interpretability. (Baryannis et al., 2019) explore the trade-off between interpretability and prediction performance, finding that a more interpretable algorithm (Decision Trees) resulted in lower accuracy than a less interpretable counterpart (Support Vector Machine). As they note, research on improved interpretability is vital to the adoption of DSCS. Relatedly, uncertainty quantification is also an imperative to decision support systems using AI methods for DSCS. Predictions and decisions made by AI algorithms need to be given with confidence intervals, to inform human decision makers whether or not the information is trustworthy. Recent research in Gaussian Processes and Bayesian Neural Networks may be worthy of further investigation in DSCS and the acceptable trade off between interpretability and performance needs to be investigated before wider adoption of AI practices in DSCS.

From a data perspective, in order to build a comprehensive risk surveillance system, companies will have to collect data from real-world operations from multiple interacting subsystems. Data sources may emanate from different platforms with non-uniform data standards. Integrating these different data sources is nontrivial, necessitating expertise in data processing, integration and maintenance. The resulting benefits need to be considered against the costs of data access and maintenance. Determination of when models need to be updated will be another important consideration.

An additional data challenge pertaining to surveillance is data imbalance, which occurs when the target of prediction is precisely where we have less data available. For example, supply chain disruptions or linkages carry imbalance (Kinra et al., 2020). In other words, when one is tasked to predict supply chain risk through digital data, one often has a plethora of supply chain data during normal operation and limited samples of disruption data, making prediction hard. While a number of approaches have been proposed to tackle this issue, more research is needed to create frameworks for DSCS specific data issues.

Another observation on the challenges we have collected in Table 1 imply that they may necessitate multiple, complementary approaches to be brought together each of which will carry a degree of uncertainty. To illustrate, consider Challenge B, where the buyer would like to know whether a supplier in its supply network is disrupted. This supplier may not be visible to the buyer, the buyer needs to first estimate that it has ties to it, making this first a network discovery problem. Next, the buyer needs to estimate that a disruption happened which might reach to it. Thus a seemingly simple challenge may necessitate an approach where different techniques need to be developed for different problem components and results brought together. The various forms of uncertainty arising from each investigatory component need to be integrated and interpreted appropriately. A combination approach will also necessitate a diverse skillset.

7. CONCLUSIONS

While surveillance of supply chains is not a new concept, digitalization offers a step change in its potential reach and scale, as large volumes of digital data and a diverse set of AI techniques to collect and analyze data become available, providing an important opportunity to help organizations fill information gaps in their supply chain. In this paper, we briefly conceptualized the emerging practice of *"Digital Supply Chain Surveillance* (DSCS)" as the proactive monitoring of digital data that allows firms to track, manage and analyze information related to a supply chain network without the explicit consent of firms involved in the supply chain. A subsequent study on existing literature mapped the extant DSCS surveillance challenges that have been proposed by researchers and industrialists, and how AI approaches may enable them. SCRM and cost reduction were identified as

domains of investigation where DSCS can benefits. We discussed technical, ethical, managerial challenges involved in the application of DSCS with AI.

Digitalizing Surveillance in Supply Chains may remove human discretion and introduce a further, hidden, bias through training data or algorithm design, that is difficult to tease out without relevant AI skill and expertise. Thus organizations that want to pursue DSCS may need to invest in AI expertise to ensure bias is removed and plan for business processes that can interpret DSCS findings and circumvent hidden bias.

We also highlighted that often a surveillance challenge may necessitate a decomposition approach, where the generic problem needs to be tackled in a step by step fashion, using different AI approaches, each of which present uncertainties, which then need to be integrated together. The application of AI to DSCS is non-trivial and further research is needed to understand which techniques are suitable for what types of problems. Data integration, imbalance, interpretability, and uncertainty quantification were also raised as important issues for the technical advancement of DSCS.

8. REFERENCES

(Roger) Jiao, J., You, X., Kumar, A. (2006). An agent-based framework for collaborative negotiation in the global manufacturing supply chain network. Robotics and Computer-Integrated Manufacturing, 22(3):239–255.

Ahmadi, B., Javidi, B., Shahbazmohamadi, S. (2018). Automated detection of counterfeit ICs using machine learning. Microelectronics Reliability, 88–90, 371–377.

Ahn, Y.Y., Ahnert, S. E., Bagrow, J. P., Barabási, A.-L. (2011). Flavor network and the principles of food pairing. Scientific Reports, 1(1):196.

Alikhani, R., Torabi, S. A., Altay, N. (2019). Strategic supplier selection under sustainability and risk criteria. Int Journal of Production Economics, 208:69–82.

Aristodemou, L., Tietze, F. (2018). The state-of-the-art on Intellectual Property Analytics: A literature review on artificial intelligence, machine learning and deep learning methods for analysing intellectual property (IP) data. World Patent Information, 55:37–51.

Astill, J., Dara, R. A., Campbell, M., Farber, J. M., Fraser, E. D. G., Sharif, S., Yada, R. Y. (2019). Transparency in food supply chains: A review of enabling technology solutions. Trends in Food Science & Technology, 91, 240–247.

Aziz, A., Kosasih, E., Griffiths, R. Brintrup, A. (2021). Data Considerations in Graph Representation Learning for Supply Chain Networks. International Conference on Machine Learning

Baryannis, G., Dani, S. and Antoniou, G., 2019. Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. Future Generation Computer Systems, 101:993-1004.

Blackhurst, J., T. Wu, P. O'Grady. 2004. Network-based approach to modelling uncertainty in a supply chain. Int Journal of Production Research 42 (8): 1639–1658

Brintrup, A., Wichmann, P., Woodall, P., McFarlane, D., Nicks, E., Krechel, W. (2018). Predicting Hidden Links in Supply Network Complexity

Harland, C., Brenchley, R. and Walker, H., 2003. Risk in supply networks. Journal of Purchasing and Supply management, 9(2), pp.51-62.

Ivanov, D., Dolgui A., Sokolov B.. 2018. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. International Journal of Production Research 0 (0): 1–18.

Juttner, U. 2005. Supply chain risk management: Understanding the business requirements from a practitioner perspective. The International Journal of Logistics Management 16 (1): 120–141.

Kinra, A., Ivanov, D., Das, A., Dolgui, A. (2020). Ripple effect quantification by supplier risk exposure assessment. International Journal of Production Research, 58(18), 5559–5578.

Kosasih, E., & Brintrup, A. (2021). A Machine Learning Approach for Predicting Hidden Links in Supply Chain with Graph Neural Networks. https://doi.org/10/325126

Kuo, R. J., Wang, Y. C., & Tien, F. C. (2010). Integration of artificial neural network and MADA methods for green supplier selection. Journal of Cleaner Production, 18(12):1161–1170.

Kuo, R. J., Wang, Y. C., Tien, F. C. (2010). Integration of artificial neural network and MADA methods for green supplier selection. Journal of Cleaner Production, 18(12), 1161–1170.

Manuj, I., J.T. Mentzer. 2008 Global supply chain risk management. J of Business Logistics 29(1):133–155.

O'Leary, D. E. (2015) Twitter Mining for Discovery, Prediction and Causality. Intelligent Systems in Accounting, Finance and Management, 22(3):227–247.

Pret allergy death: Parents 'delighted' by 'Natasha's law' plan. (2019, June 25). BBC News

Psarommatis, F., May, G., Dreyfus, P.-A., Kiritsis, D. (2020). Zero defect manufacturing: State-of-the-art review, shortcomings and future directions in research. International Journal of Production Research, 58(1)1–17.

Tang, O., S. Nurmaya Musa. 2011. Identifying risk issues and research advancements in supply chain risk management. Int Journal of Production Economics 133(1): 25–34.

Tang, Y., Liu, T., Shiy, J., Han, H., Liu, G., Dai, R., & Wang, Z. (2020). Ontology based Knowledge Modeling and Extraction of Power Equipment Supply Chain. 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), 1–5.

The Guardian (2013) Horsemeat scandal

Wichmann, P., Brintrup, A., Baker, S., Woodall, P., McFarlane, D. (2018). Towards automatically generating supply chain maps from natural language text. IFAC-PapersOnLine, 51(11):1726–1731.

Ho W., Zheng T, Yildiz H., Talluri S. (2015) Supply chain risk management: a literature review, International Journal of Production Research, 53:16, 5031-5069

Xie, M., Wang, T., Jiang, Q., Pan, L., Liu, S. (2019). Higher-Order Network Structure Embedding in Supply Chain Partner Link Prediction. Computer Supported Cooperative Work and Social Computing (pp. 3–17). Springer.

Yang, C., Sun, J. (2019). Research on Negotiation of Manufacturing Enterprise Supply Chain Based on Multi-agent. Journal of Internet Technology, 20(2):389–398.

ID	Surveillance challenge - example	Category	Stakeholders	Relevant references that mention challenge category	Approaches proposed to address DSCS Challenges
A	*If I order part a, from supplier s, it is likely to arrive 3 days late*	Supply Risk	Buyer	Harland et al 2003, Chopra and Sudhi 2004, Blackhurst et al 2008, Manuj and Mentzer 2008, Tang and Tomlin 2008, Kumar et al 2010, Tang and Musa 2011, Tummala and Schoenherr 2011, Samvedi et al 2013.	He et al 2014, Brintrup et al. 2020
B	*Supplier is disrupted with likelihood*	Supply Risk	Buyer, Insurer	Harland et al. 2003, Chopra and Sudhi 2004, Blackhurst et al 2008, Manuj and Mentzer 2008, Tang and Tomlin 2008, Kumar et al 2010, Tang and Musa 2011, Tummala and Schoenherr 2011, Samvedi et al 2013.	He et al 2014, O'Leary 2015
C	*Supplier has quality issues for product*	Quality risk	Buyer	Blackhurst, Scheibe, and Johnson 2008	Psarommatis et al.2020
D	*Buyer b is likely to be connected to suppliers in a hazardous zone*	Network related risk, risk in external environment	Buyer, Insurer	Jüttner et al. 2003, Wu et al . 2006 , Lin and Zhou 2011	Brintrup et al. 2018, Xie et al. 2019, Aziz et al. 2021, Kosasih et al. 2022, Wichmann et al. 2018,
E	*Supplier s might be supplier to buyer b*	Network related risk, risk in external environment, competitive risk	Buyer, Insurer	Jüttner, Peck, and Christopher 2003, Wu, Blackhurst, and Chidambaram 2006 , Lin and Zhou 2011 , Harland et al .2003	Brintrup et al. 2018, Xie et al. 2019, Aziz et al. 2021, Kosasih et al. 2022, Wichmann et al. 2018
F	*Supplier s might be connected to supplier k*	Network related risk, risk in external environment	Buyer, Insurer	Jüttner, Peck, and Christopher 2003, Wu et al. 2006 , Lin and Zhou 2011	Brintrup et al. 2018, Xie et al. 2019, Aziz et al. 2021, Kosasih et al. 2022, Wichmann et al. 2018
G	*My product p is likely to contain nuts*	Reputation risk, Regulatory Risk	Buyer, Insurer	Harland et al. 2003	Ahn et al. 2011
H	*This is a counterfeit product*	Reputation risk	Buyer, Regulatory	Harland et al. 2003	Ahmadi et al. 2018
I	*Supplier is unsustainable*	Environmental Risk, Reputation risk	Buyer, Insurer	Samvedi, Jain, and Chan 2013, Harland et al. 2003	N/A
J	*We cannot lend to Suppliers because it sells to disreputable buyer b*	Financial Risk	Financer	Harland et al. 2003	Martinez et al. 2019
K	*Supplier s might have financial problems*	Financial Risk	Buyer, Financer	Harland et al. 2003	Martinez et al. 2019
L	*Buyer b might have financial problems*	Financial Risk	Supplier, Financer	Harland et al. 2003	n/a
M	*Supplier has excess capacity*	Cost reduction, strategic negotiation	Buyer	n/a	n/a
N	*Supplier is likely to offer high price for this product*	Cost reduction, strategic negotiation	Buyer	n/a	Jiao et al. 2006, Boateng et al. 201
O	*Supplier is not innovative*		Buyer		Aristodemou et al. 2018, Trautrims et al. 2017
P	*Buyer is not likely to accept this bid for this product*	Cost reduction, strategic negotiation	Supplier	Yang and Sun 2019	Yang and Sun 2019

Table 1 Supply Chain Surveillance Challenges