Digital supply chain surveillance using artificial intelligence: definitions, opportunities and risks

Alexandra Brintrup, Edward Kosasih, Philipp Schaffer, Ge Zheng, Guven Demirel & Bart L. MacCarthy

Published online: 15 Nov 2023.

Submit your article to this journal 🗗

Article views: 13451

View related articles 🗗

View Crossmark data 🗗

Citing articles: 45 View citing articles 🗗

Taylor & Francis
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS | Check for updates

Digital supply chain surveillance using artificial intelligence: definitions, opportunities and risks

Alexandra Brintrup [a*], Edward Kosasih [a], Philipp Schaffer[a], Ge Zheng[a], Guven Demirel[b] and Bart L. MacCarthy[c]

[a]Department of Engineering, Institute for Manufacturing, University of Cambridge, Cambridge, UK; [b]School of Business and Management, Queen Mary University of London, London, UK; [c]Nottingham University Business School, University of Nottingham, Nottingham, UK

ABSTRACT

Digital Supply Chain Surveillance (DSCS) is the proactive monitoring and analysis of digital data that allows firms to extract information related to a supply network, without the explicit consent of firms involved in the supply chain. AI has made DSCS to become easier and larger-scale, posing significant opportunities for automated detection of actors and dependencies involved in a supply chain, which in turn, can help firms to detect risky, unethical and environmentally unsustainable practices. Here, we define DSCS, review priority areas using a survey conducted in the UK. Visibility, sustainability, resilience are significant areas that DSCS can support, through a number of machine-learning approaches and predictive algorithms. Despite anecdotal narrative on the importance of explainability of algorithmic results, practitioners often prefer accuracy over explainability; however, there are significant differences between industrial sectors and application areas. Using a case study, we highlight a number of concerns on the unchecked use of AI in DSCS, such as bias or misinterpretation resulting in erroneous conclusions, which may lead to suboptimal decisions or relationship damage. Building on this, we develop and discuss a number of illustrative cases to highlight risks that practitioners should be aware of, proposing key areas of further research.

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 the 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 (Christopher and Lee 2004). However, proactive, data-driven identification and monitoring of emerging risks is still a challenging area, causing significant concern to industry (Ho et al. 2015; Ivanov et al. 2017; MacCarthy, Ahmed, and Demirel 2022; Wang, Tiwari, and Chen 2017). Recent 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, Dolgui, and Sokolov 2019). A number of recent legislative initiatives make SCRM even more

pressing-imports around the world. In the United States, the Uyghur Forced Labour Prevention Act has gone into effect on 21 June 2022. US Customs and Border Protection has issued Withhold Release Orders for goods originating from parts of the world with a high risk of forced or child labour. Similarly, in Europe supply chain laws including the EU Green Deal and Germany's Supply Chain Due Diligence Act will require companies to disclose the source of their raw materials and ask for reassurance that their supply chain partners are not taking part in environmentally harmful practices or abuses of human rights. In the UK, the Transparency in Supply Chains Provision of the Modern Slavery Act (MSA) requires companies with an annual turnover of £36 m or more to report annually on their actions to identify, prevent and mitigate modern slavery in their supply chain. Traceability and compliance with California Supply Chain Transparency Act, UK Modern Slavery Act, Conflict Minerals Regulation that came to full force on 1 January 2021 ask companies in the EU to source tin, tantalum, tungsten and gold responsibly, and show that their

---

procurement does not contribute to political conflict or illegal activities.

Typical approaches to identify these risks include customer surveys, accreditation approaches, manual mapping and monitoring of suppliers, and third-party auditing services, which tend to be costly, and require significant effort and time investment (MacCarthy, Ahmed, and Demirel 2022; Wichmann et al. 2018). Christopher and Peck (2004) highlight that a 'fundamental pre-requisite for improved supply chain resilience is an understanding of the network that connects the business to its suppliers and their suppliers and to its downstream customers. Mapping tools can help in the identification of "pinch points" and "critical paths"'. Several other authors have since noted the link between improved supply chain visibility and effective risk management (Basole and Bellamy 2014). However, according to industrial surveys '40% of companies who sourced only in the UK, and almost 20% who sourced globally, had no supply chain information beyond their direct suppliers', and data and visibility is a critical differentiator for effective risk management (EY, Ernst and Young 2020).

A number of recent studies show that Supply Chain Digitalisation might offer companies a set of additional approaches to complement extant methods to address the visibility 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 (e.g. for a review, please see Ivanov, Dolgui, and Sokolov 2019). 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 through improved visibility.

Within the scope of this paper, we adopt the broader definition by Barratt and Oke (2007), who have defined supply chain visibility as 'the extent to which actors within the supply chain have access to or share timely information about supply chain operations, other actors and management which they consider as being key or useful to their operations'. 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 potentially more informative. Whilst the use of Artificial Intelligence (AI) is not a strict prerequisite to analyse digital data, the vast majority of methods we review in this paper use some form of AI, as it provides performance improvements over other methods in dealing with unstructured, large-scale digital data automatically. At the same time, relying on automated surveillance may carry risks without appropriate mechanisms to validate datasets and algorithms used, especially if they are proprietary.

In this paper, we define and explore the newly emerging field of Digital Supply Chain Surveillance (DSCS) and discuss the role of AI in it through a sequential mixed-methods design which utilises a literature review, use case illustrations, a survey instrument and a quantitative case study. We first review and categorise extant literature, the types of surveillance activities that are currently being proposed and attempted by DSCS, and the common data sources and AI methods that are used (Section 2). This is followed by an analysis to identify risks posed by the use of AI in DSCS practice, with illustrative use cases (Section 3). We then deploy an industrial survey within the UK to explore the areas, methods and the extent to which UK-based companies gather supply chain intelligence, importance of different surveillance challenges and the criteria with which surveillance performance is evaluated (Section 4). Binomial and logistic regression models are used to explore the uptake of DSCS by the UK industry using quantitative survey data ($N = 62$). Finally, a case study investigates one of the most popular DSCS areas in literature that of supply chain risk, where we apply the methods proposed to explore their efficacy. The explanatory sequential design helps us integrate findings, highlight some of the challenges and pitfalls that need to be further researched within this area (Section 5).

2. Digital supply chain surveillance: background and definitions

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. Researchers agree that the 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 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 and (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. Artificial Intelligence (AI), also called Machine Intelligence or Computational Intelligence, is used to describe machines that mimic and improve human cognitive functions that we associate with human intelligence, such as learning and problem solving (Russell and Norvig 2009). In the context of DSCS, the human whose behaviour is mimicked is an SC professional that searches for and assesses information on a company's supply chain. While AI is not a strict prerequisite for DSCS, all three phases benefit from AI's ability to acquire and process large volumes of digital data in an automated manner, the extent of which would not have been possible to undertake manually. Moreover, AI has recently been shown to have had positive impacts across many use cases in supply chain, helping supply chain practitioners search and assess information that are useful to respond the dynamic environment (Cannas et al. 2023; Dohale et al. 2022; Sharma 2023). 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. Our recent studies showed that this type of data can be used to

predict supplier delays or even possible relations between suppliers (Brintrup et al. 2018; Zheng, Kong, and Brintrup 2023). Data that is externally available may consist of social media, company annual reports and news outlets and even phone, shipment and postal records, as well as the emerging metaverse (Dolgui and Ivanov 2023), 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. Brintrup et al. (2022) outline the broader supply chain management context for the emerging field of AI-driven surveillance.

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?' Second, 'Which stakeholders are interested in different surveillance challenges?' and finally, 'What are the challenges involved in the application of DSCS?'. We review these next through synthesising both a literature review (Section 2), illustrative cases (Section 3) and a survey based analysis within the UK (Section 4) as well as an in-depth case study to show how DSCS can be used (Section 5).

2.2. Surveillance challenges and digital solution approaches reported in the literature

The first steps in DSCS have included the detection of fraudulent supply chain transactions (Zage, Glass, and Colbaugh 2013), social media monitoring for disruptions (O'Leary 2015), supply chain data mining from the web (Wichmann et al. 2018), prediction of dependencies (Brintrup et al. 2018). Most efforts on DSCS have been on improved visibility with a view to improve resilience against disruptions. While the area is still emerging, recent government initiatives (ONS 2022), the diversity of topics it aims to address (Table 1) and the number of start-up companies reviewed in Section 2.3 point to DSCS as an area that deserves scholarly attention.

Table 1 shows various supply chain surveillance challenges that have been identified following extant supply chain risk categorisations from the literature 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

Table 1. Supply chain surveillance challenges.

ID	Surveillance challenge – example	Category	Stakeholders	Relevant references that mention challenge category	Approaches proposed to address DSCS Challenges	Data sources used	AI methods used
A	If I order part a, from supplier s, it is likely to arrive 3 days late	Resilience	Buyer	Harland, Brenchley, and Walker (2003), Blackhurst, Wu, and O'Grady (2004); Manuj and Mentzer (2008), Tang and Tomlin (2008), Tang and Nurmaya Musa (2011), Tummala and Schoenherr (2011), Samvedi et al. (2013)	He et al. (2014), Brintrup et al. (2020), Zheng, Kong, and Brintrup (2023)	ERP data	Classification (Naïve Bayes, Support Vector Machine, Gradient Boosting, Decision Trees) Regression (Neural network)
B	Supplier is disrupted with likelihood	Resilience	Buyer, Insurer	Harland, Brenchley, and Walker (2003), Blackhurst, Wu, and O'Grady (2004); Manuj and Mentzer (2008), Tang and Tomlin (2008), Tang and Nurmaya Musa (2011), Tummala and Schoenherr (2011), Samvedi, Jain, and Chan (2013)	He et al. (2014), O'Leary (2015)	Social media	Natural Language Processing
C	Supplier has quality issues for product	Product quality	Buyer	Blackhurst, Scheibe, and Johnson (2008)	Psarommatis et al. (2020)	ERP data, maintenance logs	Classification (Neural Networks)
D	Buyer b is likely to be connected to suppliers in a hazardous zone	Resilience	Buyer, Insurer	Jüttner, Peck, and Christopher (2003), Lin and Zhou (2011)	Brintrup et al. (2018), Xie et al. (2019); Aziz et al. (2021), Kosasih and Brintrup (2021a), Wichmann et al. (2018), Kosasih and Brintrup (2021b)	World Wide Web, industrial databases, annual reports	Natural Language Processing, Classification (Neural Networks) Knowledge Graph Completion, Neuro Symbolic AI
E	Supplier s might be supplier to buyer b	Visibility, Resilience, Competition	Buyer, Insurer	Jüttner, Peck, and Christopher (2003), Lin and Zhou (2011), Harland, Brenchley, and Walker (2003)	Brintrup et al. (2018), Xie et al. (2019); Aziz et al. (2021), Kosasih and Brintrup (2021a); Wichmann et al. (2018), Kosasih and Brintrup (2021b)	World Wide Web, industrial databases, annual reports	Natural Language Processing, Classification (Neural Networks) Knowledge Graph Completion, Neuro Symbolic AI
F	Supplier s might be connected to supplier k	Visibility, Resilience	Buyer, Insurer	Jüttner, Peck, and Christopher (2003), Lin and Zhou (2011)	Brintrup et al. (2018), Xie et al. (2019); Aziz et al. (2021), Kosasih and Brintrup (2021a); Wichmann et al. (2018), Kosasih and Brintrup (2021b)	World Wide Web, industrial databases, annual reports	Natural Language Processing, Classification (Neural Networks) Knowledge Graph Completion, Neuro Symbolic AI
G	My product p is likely to contain nuts	Product quality	Buyer, Insurer	Harland, Brenchley, and Walker (2003)	Ahn et al. (2011)	Food retail datasets	Classification (Neural Networks), Clustering
H	This is a counterfeit product	Product quality	Buyer, Regulatory	Harland, Brenchley, and Walker (2003)	Ahmadi, Javidi, and Shahbazmohamadi (2018)	N/A	Classification (Neural Networks)
I	Supplier is unsustainable	Sustainability	Buyer, Insurer	Samvedi, Jain, and Chan (2013), Harland, Brenchley, and Walker (2003)	N/A	Carbon emission reporting	Classification (Neural Networks)

Table 1. Continued.

ID	Surveillance challenge – example	Category	Stakeholders	Relevant references that mention challenge category	Approaches proposed to address DSCS Challenges	Data sources used	AI methods used
J	*We cannot lend to Suppliers because it sells to disreputable buyer b*	Financial	Financer	Harland, Brenchley, and Walker (2003)	Martinez et al. (2019)	Financial records, World Wide Web, industrial databases, annual reports	Natural Language Processing
K	*Supplier s might have financial problems*	Financial	Buyer, Financer	Harland, Brenchley, and Walker (2003)	Martinez et al. (2019),	Financial records	Natural Language Processing
L	*Buyer b might have financial problems*	Financial	Supplier, Financer	Harland, Brenchley, and Walker (2003)	n/a	Financial records	Natural Language Processing
M	*Supplier has excess capacity*	Negotiation	Buyer	n/a	n/a	Shipment records, ERP data	
N	*Supplier is likely to offer high price for this product*	Negotiation	Buyer	n/a	Jiao, You, and Kumar (2006), Boateng et al. 2017	Spenditure data	Classification
O	*Supplier is innovative*	Innovation	Buyer	Aristodemou et al. (2018), Trautrims et al. (2017)	Aristodemou et al. (2018), Trautrims et al. (2017)	Patents	Neural networks
P	*Buyer is not likely to accept this bid for this product*	Negotiation	Supplier	Yang and Sun (2019)	Yang and Sun (2019)	Sales records	Multi-agent learning

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.

Challenges A and B relate to the *Risk and Resilience*. 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, Dani, and Antoniou (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. Zheng, Kong, and Brintrup (2023) apply federated learning to the same problem wherein multiple buyers update a common prediction model on their common suppliers. Their approach showed that even firms with little or no historical data on suppliers can make useful predictions by tapping into collective knowledge, without the risk of exposing their confidential data.

Challenges D, E and F pertain to *Visibility* 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. The lack of visibility remains a significant challenge for companies. Several studies have shown how the 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) analysed 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 and Brintrup (2021a) created a Graph Neural Network that considers only topological features, reporting improvements over Brintrup et al. (2018). Kosasih and Brintrup (2021b) and 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. Brockmann, Elson Kosasih, and Brintrup (2022) proposed an ensembled graph neural network approach to augment predicted links with uncertainty scores to support real-world decision-making.

Challenges C, G and H are related to surveilling a supplier's *Product Quality*. 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 and Heide 2015) and nut allergies in sandwiches ('Pret Allergy Death' 2019). Similar issues may be observed in toys where toxic ingredients have been discovered. 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 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 analysing online transaction data to detect fraudulent vendors artificially building a good reputation through fake online reviews.

Challenge I focuses on *Sustainability*. 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, Torabi, and Altay 2019) through the use of DSCS. For instance, Kuo, Wang, and Tien (2010) explored the interests and rights of employee (IRE) and the rights of stakeholders (RS), Azadnia et al. (2015) studied long-term stability, Chiou et al. (2008) investigated Environmental Management Systems whereas Klassen and Vereecke (2012) studied the management of social issues such as child labour, health, safety and discrimination.

Challenges J, K and L are concerned with the *Financial* surveillance on the supply chain. Here a buyer may be 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 surveillance to support procurement *Negotiation*. Many supply chain actors negotiate contracts with large lists of suppliers and buyers dispersed globally. While procurement officers will often manually analyse price negotiation opportunities, DSCS may help provide automated ways to find patterns in pricing to make negotiation more efficient, especially in settings where the scale of analysis and number of suppliers is too large to manually handle (Lee 2021). Researchers have been exploring several techniques such as multi-agent systems to model pricing likelihood and optimized agreements between suppliers and buyers (Jiao, You, and Kumar 2006, Boateng et al. 2017) based on historical data on supplier prices. Lee (2021) has proposed the use of machine learning to detect bid anomalies and predict bids, so as to facilitate negotiation with a-priori data. Swartz et al. (2019) proposed observing shipping container volumes and descriptions to extract the volume of transactions for predicting the capacity of suppliers and supply chain dependencies, which can aid in negotiation.

Challenge O is about supplier *Innovation*, which is a significant supplier selection criterion in industries that undergo frequent innovative disruptions. 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

Table 2. Current commercial solutions offered for DSCS.

Company	Category	Description
Sourcemap https://sourcemap.com	Visibility, Resilience, Sustainability	Tool to ask suppliers to share sub-tier information, which then allows a snowballing process. DSCS concentrates on the application of AI to automatically query public compliance databases and proprietary risk databases
Resilinc https://www.resilinc.com	Visibility, Resilience	EventWatch solution that monitors news for a given set of suppliers, and a multi-tier mapping solution which collects data from the web, bills of lading, and press releases
Everstream Analytics https://www.everstream.ai/	Visibility, Resilience, Sustainability	News monitoring with Natural language processing, connects to ERP data, and proprietary data sources
ImportGenius https://www.importgenius.com	Negotiation	Allows tracking of competitor's shipments and supplier to identify prospect buyers. Allows companies to monitor public companies' imports and exports and identify market trends and predict on the success or failure of new product launches. Uses ocean freight records
Altana AI https://www.altana.ai	Visibility, Resilience	Attempts to federate different data streams from shipments and bills of lading with HS codes, and extracts company relationships with Natural Language Processing. Uses predictive algorithms for entity resolution (which company does a given shipment record refer to) and predicting what is inside a shipment container and its volume and associated value. Resolves time lags with 'nowcasting' to predict who supplies whom. Provides a shipment rating for customs compliance. Founders are former-Panjiva employees
Panjiva https://panjiva.com	Visibility, Resilience	Uses government data sources with freedom of information requests. Uses shipment data, public and private subscription company data, port of lading data. Acquired by S&P Global
S&P Global Market Intelligence https://www.spglobal.com/	Financial	Prediction of financial health, using proprietary data sources. Uses Panjiva's technology to report n Supply Chain Intelligence
VersedAI https://www.versed.ai	Visibility, Resilience	Built on technology initially proposed by Wichmann et al. (2018). Uses publicly available web data to train classifiers and automatically maps supply chains
HICX https://www.hicx.com	Resilience, Sustainability	Solution to consolidate Enterprise-wide supplier data with ERP based performance data to make predictions on supplier experience and performance
MakerSite https://makersite.io	Visibility, Resilience, Sustainability	After obtaining product composition and first tier supplier datasets, connects to proprietary databases to obtain sub-tier information
FRDM https://www.frdm.co	Resilience	Uses purchasing data from a company's ERP, to automatically map the first tier supply chain. Juxtaposes media alerts on the extracted map for ongoing risk alerts using Natural language processing tools
OpenSC https://opensc.org	Sustainability	Focussed in food production. Verifies ethical and sustainable practices on the supply chain such as fair payments to farmers, fishing sustainably. Uses block chain and RFID scans to collect information so not entirely independent of supplier consent. The use of DSCS technology concerns the verification stage with GPS tracking. Here if a vessel was fishing in a protected area by looking at its GPS locations, coordinated with protected zones, the vessel's speed, sea depth

suppliers (Aristodemou and 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, to enable DSCS to be automated (see Table 1 for a list of methods used). AI, at the same time, brings about a number of challenges itself. We shall discuss these later on.

2.3. Commercial offerings

In this section, we briefly review companies offering solutions that enable DSCS. We deliberately exclude solutions that involve supplier surveying, and inviting suppliers to use block chain or other tracking systems, as all of these depend on the willingness of suppliers to share data, therefore remain outside the remit of 'surveillance'. Table 2 displays the current landscape of solutions offered.

Commercial solution providers we review mainly focus on natural language processing to extract, resolve and identify suppliers and merge shipment data with data from the web. Some collate industrial databases, offer media monitoring to identify potential disruptions, and some have built analytics capability to identify supplier concentration and risk. A number of these have been formed after being acquired from each other. It is interesting that almost all companies focus on a small subset of the DSCS categories outlined in Table 1, but various others such as innovation, product quality, competition have been neglected. Most companies focus on visibility, resilience and sustainability. Majority of these companies thus focus on similar solutions, built on similar datasets, though the precise underlying algorithms are harder to assess as they are proprietary. Being so, they may pose risks if companies over-rely on their use, as the trustworthiness of underlying datasets or algorithmic inferences cannot be scrutinised. It is also worth noting that there is a concentration of US-based companies with European

Table 3. Regression models.

Model type	Dependent variable	Independent Variables
BLR – Model 1	Use of internal datasets	Sector, Size, Complexity*, International, Visibility
BLR – Model 2	Use of social media	Sector*, Size, Complexity, International, Visibility
BLR – Model 3	Use of supplier websites	Sector, Size·, Complexity*, International, Visibility
BLR – Model 4	Use of search engine	Sector, Size, Complexity, International, Visibility**
BLR – Model 5	Use of external audit companies	Sector, Size, Complexity·, International**, Visibility·
BLR – Model 6	Use of business intelligence software	Sector·, Size·, Complexity·, International, Visibility·
BLR – Model 7	Use of artificial intelligence	Sector*, Size, Complexity, International, Visibility
OLR – Model 1	Level of automation	Sector*, Size·, Complexity·, International, Visibility
OLR – Model 2	Proportion of intelligence gathering on suppliers	Sector*, Size, Complexity, International, Visibility·
OLR – Model 3	Regularity of intelligence gathering	Sector*, Size, Complexity·, International, Visibility
OLR – Model 4, 5, 6	Delays, Excess Capacity, Quality, Price	Sector*, Size, Complexity·, International, Visibility
BLR – Model 8	Explainability (overall)	Sector*, Size*, Complexity*·, International, Visibility*
BLR – Model 9	Explainability (supplier performance)	Sector*, Size, Complexity, International, Visibility*
BLR – Model 10	Explainability (demand forecasting)	Sector*, Size, Complexity, International, Visibility
BLR – Model 11	Explainability (delay prediction)	Sector*, Size, Complexity, International, Visibility*

. $= P < 0.1$, * $= P < 0.05$, ** $= P < 0.01$, *** $= P < 0.001$

companies being two spin offs from funded research projects (namely, Versed.ai and MakerSite).

3. Discussion on the risks of AI-based DSCS and illustrative use cases

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 (Wichmann et al. 2018). 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 may remove human discretion but introduce further hidden biases from the training data used or from algorithm design. A bias in an artificial intelligence system is defined as any preference or inclination influencing the algorithm's decision-making. Thus bias occurs when an algorithm is trained to prefer some outcomes over others.

Bias may be difficult to tease out without relevant AI skill and expertise. Lianos and 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.

Bias could typically result from data imbalance, which refers to one or more features in a training dataset are severely under or over represented. This may happen through selective sampling, genuine data imbalance or through feature engineering, where features that are biased are unintentionally added to the data. When there is not enough data to properly train a given model, the model may start to make connections that are not really there. For example, when predicting supply chain disruptions occurs one often has a plethora of supply chain data during normal operation and limited samples of disruption data, making prediction hard, when the target of prediction is precisely where we have less data available. The features that occur during a disruption may be spuriously associated with one or more input features that present coincidentally. A number of approaches have been proposed to tackle this issue, including data cleaning algorithms, oversampling and undersampling to increase the representation of infrequent observations. Weighting samples or features may help modify the relative significance of individual cases. Post-hoc analysis can help evaluate prediction bias and adjust algorithms as needed. More research is needed to identify and create frameworks for bias in DSCS practice.

> *Illustrative Use Case 1: Hidden bias in data*
> A company wishes to predict sustainability scores for companies involved in its supply chain. It purchases a dataset that includes sustainability score samples from a number of companies in different parts of the world. The prediction algorithm flags up a long-term, high-performing supplier with operations in New Zealand. Upon further inspection it is found that New Zealand is severely underrepresented in the industry sample that was purchased (3 out of 1000 companies). The few companies that existed in the data sample had either received incomplete sustainability scores or were not highly performing in sustainability, which has affected this company's predicted score.

Incorrect data might be a significant issue in DSCS, particularly when predicting disruptions or sustainability of suppliers. An obvious source of incorrect data would occur when monitoring social media for news. As we have seen, news have been an important source of DSCS, the monitoring of which is now offered by commercial DSCS companies. While social media is low cost and easy access, it also contains low quality or even intentionally incorrect information. The detection of misleading, incorrect information is an active area of research in the AI community, which should be adopted by researchers and practitioners alike. Updating models at the right time is another important consideration, especially in cases where the correctness of predictions may be impacted over time. For example predictions on supplier delivery with data obtained during the Covid-19 period might not yield relevant results post pandemic.

Other sources of incorrect data in DSCS might simply be in the form of errors, such as sensor faults, for example to detect storage conditions or location of items, or might come from business practices as shown by the illustrative case below, which may be harder to detect. In such situations, practices for monitoring data collection need to be put into place, to differentiate genuine trends from those that are caused by incorrect data collection.

> *Illustrative Use Case 2: Incorrect input data*
> A company analyses supplier delivery performance using warehouse delivery data. The supplier always seems to be late when it is tasked to deliver on Fridays. Further analysis shows that the delivery company scheduled the delivery on Friday 5:30 pm, when warehouse shift ends. Any deliveries that are received beyond this point are temporarily held in a buffer zone, and logged in on Monday morning, even if they have arrived on time.

The uncertainty of a prediction adds a critical layer of transparency for safe deployment and use. Hence DSCS challenges will benefit from uncertainty quantification to inform human decision makers whether or not the information is trustworthy.

In addition, many of the DSCS challenges highlighted in Table 1 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 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 Visibility problem. Suppose the buyer purchases software which predicts the presence of a second tier supplier connected to this buyer. Next, the buyer is alerted to the news that a disruption happened at this particular supplier. Here, the buyer needs to explore the possibility of this disruption effecting it, my combining multiple uncertainties: one which is associated with the supplier being indeed a part of its network, one where a disruption has actually happened within the supplier and finally, one associated with the probability of this disruption cascading through the network to the buyer. 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.

> *Illustrative Use Case 3: The need for uncertainty*
> A buyer has received some news that a devastating earthquake happened in Tokyo, Japan. The buyer does not have any direct suppliers there, but has a subscription to an automated supply chain mapping software which predicts that one of its suppliers is connected to a company in Tokyo. The buyer panics and calls its supplier who reassures him that no such connection exists. It turns out that the software has predicted a connection to Tokyo because of a recent merger, with a company that is headquartered in Tokyo, but has no actual production there. The problem of identifying companies and differentiating between legal entities and production location is a significant issue in automated supply chain mapping software. The buyer is left wondering whether to trust such mapping software.

Linked with uncertainty is the question of explainability of AI. Many state-of-the-art AI algorithms are 'black box' methods, which mean 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 DSCS is interpretability. (Baryannis, Dani, and Antoniou 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. 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.

Illustrative Use Case 4: The need for explainability
A bidding prediction system is used to analyse suppliers' past bids, to estimate bidding prices and detect anomalies. A neural network is deployed to predict prices with high accuracy, however, the buyer wanted to know what the main pricing determinants were. The analyst then conducted a decision tree-based method, which was inherently more explainable. Initially, data pertaining to all parts bought through the bidding process were used. Subsequent feature analysis showed that suppliers were the main determinant of prices, leading the company to conclude that it needed to be tougher during negotiations. After the announcement of conclusions at the management meeting, a chance conversation between the chief design engineer and the procurement officer took place, where it was discussed whether actually it was part geometric complexity that was driving prices. A subsequent analysis was performed, dividing parts into categories of increasing geometric complexity, where it was found that in higher priced products, bids were determined by complexity. Furthermore, suppliers that were offering high complexity parts were different to those offering lower complexity parts, misleading the algorithm to infer supplier choice determined bid prices.

Use cases that DSCS may facilitate but are not a part of traditional supply chain management practices, 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 has typically not been visible to a buyer. Similarly, a supplier may now use historical payment data to predict whether a buyer will pay on time.

It is important to design processes that handle new information with care, leading to appropriately balanced action. Graham and 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, the prediction of certain events or trends needs to be handled carefully and with balance.

Illustrative Use Case 5: Incorporating DSCS results into procurement practice
A company that produces and leases heavy machinery recently has recently set up an analytics team which undertook several initiatives. One of these is a programme that deployed sensors on its machines, to predict when parts may fail. The team also developed a defective parts per million (DPPM) software to estimate the quality of goods received from suppliers.

After a certain amount of time, it is realised that there is significant discrepancy between parts ordered for manufacture and spare parts available for maintenance operations. The company needs to renegotiate volumes with its parts suppliers and merge the DPPM estimation output and the prognostics system with its ERP to re-establish the process for determining its economic order quantities.

DSCS may face challenges regarding privacy. First of these is the potential loss of control of private data. Although datasets that are used in various DSCS applications may be based on publicly available sources, inferences that are made using publicly available data might be private. Although one might argue that the point of pursuing surveillance would be to identify such dependencies, doing so may be detrimental to buyer–supplier relationships. As companies adopt AI for supply chain business intelligence more research will need to be conducted on best practices for managing and handling sensitive data and its impact on supplier relationship management.

Appropriate safeguards must be in place to maintain privacy and access to data. Several commercial offerings do not state where they have obtained their datasets from, but mention unknown 'proprietary sources'. This not only highlights a trust issue, as a company purchasing DSCS services may not know with certainty the truthfulness of obtained information and its relevancy at the time of making inference but also a legal issue as datasets may be used in jurisdictions they do not originate from. Similar to other domains such as healthcare, monetisation of supplier data may mean that private custodians of

data can be influenced by competing goals and should be structurally encouraged to ensure data protection (Murdoch 2021).

> *Illustrative Use Case 6: Privacy breech*
> Through automated supply chain mapping software, a company learns that it is connected to a second tier supplier in a certain location which provides certain rare minerals. Using this prediction, the company identifies one of its direct suppliers which buys from the mining company as it knows that the product that it purchases contains those minerals. The buying company uses this opportunity to renegotiate contract when it learns about surplus of the second tier supplier. The direct supplier feels that its confidential information has been breached and terminates the contract.

In addition to the above, a comprehensive DSCS system typically entails collection of data from multiple sources, which 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. As our survey shows, many companies prefer to deploy internal analytics teams to perform DSCS. The resulting benefits need to be considered against the costs of data access and maintenance.

4. A survey of digital supply chain surveillance in the UK

In this section, we report on the results of a UK-based survey that was conducted to explore the use of DSCS by practitioners. The aims of the survey were to:

(1) Explore the areas, methods and the extent to which UK based companies gather supply chain intelligence
(2) Rank the importance of different surveillance challenges, and the criteria with which surveillance performance is evaluated.

We additionally investigated the relationship between supply chain intelligence gathering practices, and supply chain size, complexity and industrial sector that varied between the participants (Figure 1). We define supply chain size as the number of companies involved in the supply chain of the surveyed company respondent. Complexity variable encapsulates vertical (number of tiers) and horizontal (number of suppliers per tier) complexities following Bode and Wagner (2015).

The survey involved 62 respondents from Manufacturing (61.2%) and Services (38.8%). Manufacturing sectors include: Pharmaceutical, Machine Tooling, Automotive, Aerospace, Maritime engineering, Defence, Food and Agriculture, and Energy, whereas Services industry
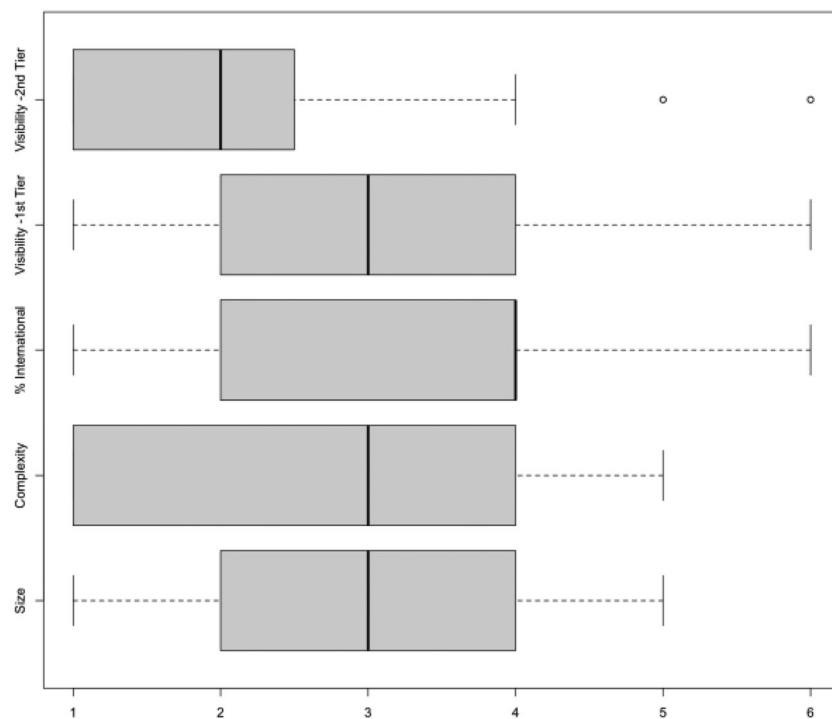
Figure 1. Supply chain properties of companies that were surveyed.

included Software, Logistics and Insurance providers. All respondents were UK based. Approximately $\frac{3}{4}$ respondents were approached during the UK Digital Manufacturing Week, which has taken place during November 2022, in Liverpool, with the rest having been interviewed in person and via online meetings using a structured questionnaire instrument.

Binomial and ordered logistic regression models were used to derive the relationship between supply chain properties (Figure 1) and intelligence gathering practices (Table 1). Binomial logistic regression (BLR) models predict the probability with which an observation will falls into one of two categories of a dependent variable based on one or more independent variables. We use binomial logistic regression to explore the use of different intelligence gathering tools as a factor of supply chain complexity, visibility, company sector and size. On the other hand, ordered logistic regression (OLR) is another sub-type of logistic regression where the dependent variable is meaningfully ordered. In our case, OLR was applied to extract the relationship between supply chain characteristics and automation levels within a company's supply chain intelligence gathering processes. In what follows, we summarise survey results.

4.1. Supply chain intelligence gathering

In this section, participants were inquired about the areas in which they gathered supply chain intelligence. Only 44% of companies surveyed mentioned they gathered supply chain intelligence actively. Those that did gathered intelligence mostly on Sustainability (74%), and Innovation (74%), followed by Financial health (73%), for increased supply chain visibility (62%) and for evaluating supply chain risk and resilience (51%). In contrast a desire to find out about competing buyers was not highly ranked (31%) (Figure 2a).

Of those companies that did gather intelligence, the most popular sources of information included: internal datasets such as ERP and procurement systems (80%), followed by supplier websites (78%), business databases (58%). About half (20% of overall sample) used business intelligence software and social media. 27% used external auditing companies to gather intelligence (Figure 2b).

Companies that had complex supply chains were more likely (BLR – Model 1) to use internal datasets. Service sector preferred the use of Social media more than manufacturing sector (BLR – Model 2), Companies also actively monitored websites of suppliers when the Size and Complexity of supply chain increased (BLR – Model 3). Search engines were used to gather visibility on the third tier suppliers when supply chain visibility was low (BLR – Model 4).

The use of external audit companies was influenced by increased supply chain complexity, proportion of international suppliers and lack of visibility (BLR – Model 5)

Similarly, the use of business intelligence software was influenced by increased supply chain size and complexity and lack of visibility (BLR – Model 6). Services sector was more likely to use business intelligence software and artificial intelligence than the manufacturing sector (BLR – Model 7).

Approximately 35% of the respondents said they performed manual intelligence gathering, while 42% said intelligence gathering was semi-automated. When prompted, this meant that data that was already in-house (such as ERP data) was repurposed to extract supplier performance evaluation. Hence business intelligence gathering almost always involved the generation of internal metrics, followed by repurposing existing datasets or interpreting business intelligence software results.

OLR was applied to extract the relationship between supply chain characteristics and automation levels in supply chain intelligence gathering. It was found that companies the services sector was more likely to automate their supply chain intelligence gathering activity. Companies with smaller supply chains were more likely to perform manual intelligence gathering. Supply chain complexity also increased the likelihood of manual intelligence gathering activities (OLR – Model 1).

Of the respondents that declared they gathered supply chain intelligence, 70% said they collected information on all or most of their direct suppliers, whereas 30% said they prioritised a subset of suppliers for intelligence gathering. Manufacturing companies were more likely to gather intelligence on subsets of their suppliers which was more likely when visibility beyond their second tiers was low (OLR – Model 2).

Of the companies who actively gathered supply chain intelligence, 25% used at least one of the technologies displayed in Figure 2(c). Statistical techniques and machine intelligence were amongst the most popular technologies used. Participants highlighted that automated intelligence gathering was expensive to set up and raised questions on the authenticity of data.

Most companies (59%) analysed supply chain intelligence data using an in-house analytics team. 19% bought analytics as a service and 22% did not analyse the data gathered but stored it only.

Several companies highlighted the challenge of ingesting large amounts of supplier performance data and the lack of IT infrastructure to do so. Legacy IT architectures were mentioned as a key barrier to conducting surveillance analytics.
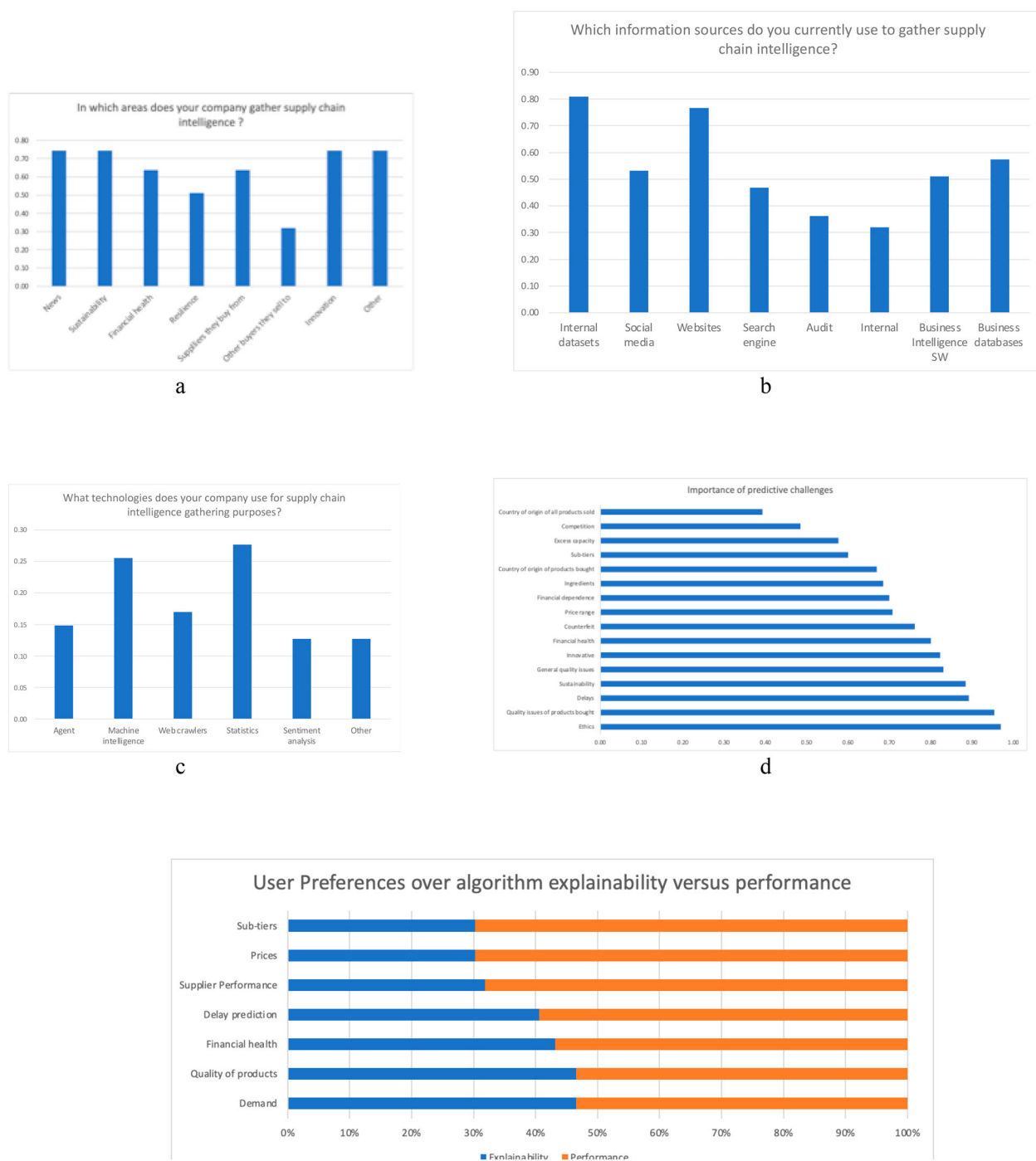
Figure 2. Illustration of digital supply chain surveillance survey responses.

Most companies surveyed have gathered supply chain intelligence as a one-off exercise (51%), with about a third conducting intelligence gathering regularly (34%). 16% of companies surveyed conducted real-time intelligence gathering. The services sector was more likely to conduct regular intelligence gathering and the manufacturing sector was more likely to have irregular, one-off initiatives as needed. Increased supply chain complexity made one-off initiatives more likely to be carried out (OLR – Model 3)

4.2. Popular surveillance challenges and success criteria

In this part of the survey, we asked respondents about the importance of different surveillance challenges outlined in Section 2.2, and success criteria associated with algorithmic approaches addressing them.

Figure 2(d) shows the importance of surveillance challenges to respondents in ranked order. Overall, the

ethical practices of suppliers (such as exploitative practice), quality issues, delays and sustainability were ranked highly. Respondents from the Manufacturing sector were more likely to rate predictions of Delays, Excess capacity, Quality issues and Price offers highly compared to the Services sector. This increased when their supply chains were rated as highly complex (BLR – Models 4–6). Several companies mentioned additional surveillance challenges they would like to pursue. These included: geopolitical risk such as regulatory and sanctions, exposure to commodities, raw materials and currency fluctuation.

When prompted about algorithmic evaluation criteria applied to surveillance challenges, overall participants rated explainability and performance over the ability to handle large-scale data. Algorithm performance was rated higher than explainability in all predictive challenges; however, the importance of explainability differed significantly, both between sectors and between predictive challenge categories.

Manufacturing sector overall preferred explainability over algorithmic performance (BLR – Model 8). Increased complexity of the supply chain made it more likely for respondents to choose explainability over algorithmic performance (BLR – Model 8).

Manufacturers were 2.85 times more likely to choose explainability over performance than services sector, holding constant all other variables. Small supply chain size (by a factor of 1.8), increased complexity (1.88) and higher visibility (2.1) were other significant factors in choosing explainability over algorithm performance (Results obtained via proportional odds logistic regression, BLR – Model 8).

Manufacturers preferred explainability especially in the prediction of supplier performance (BLR – Model 9) but not so in demand forecasting (BLR – Model 10). Interestingly, when supplier visibility is high, respondents preferred explainability in delay (BLR – Model 11) and performance prediction (BLR – Model 9). This may be due to manufacturers increased knowledge over suppliers making it more likely to want to know why a low performance is predicted by an algorithm.

5. Illustrative case study: digital surveillance for supply chain risk identification

In this section, we illustrate how to combine several approaches in DSCS to extract insights. From Table 1, our case study example can be categorised under *Challenge E*, where an insurer would like to increase visibility over dependencies in an industry and identify highly connected suppliers. Following previous studies which have explored supply chain complexity metrics for risk

evaluation (Brintrup et al. 2018, Ledwoch et al. 2018), we choose the aerospace industry as our contextual domain.

We first use the BERT-based Natural Language Processing model (Devlin et al. 2018; Wolf et al. 2020), to train a classifier for extracting and detecting supplier-buyer relationships from Reuters news articles (Wichmann et al. 2018). The resulting dataset is then converted into a knowledge graph where nodes represent companies and links represent supplier–buyer relationships between them. Subsequently, a Graph Neural Network-based Link Prediction model has been trained to identify hidden links in the graph between the companies identified following Kosasih and Brintrup (2021a). Lastly, we use systemic supply chain risk metrics proposed by Ledwoch et al. (2018) and Brintrup et al. (2018) to highlight companies that play critical role in the supply chain. In what follows we describe these steps in further detail (Table 3).

Dataset. The identified dataset to extract information on the aerospace industry was Reuters News Articles. we selected multiple data sources including the Reuters corpora TRC2 and RCV14, and the NewsIR16 datasets. To filter documents by company names, as a list of the top 100 global aerospace companies were used and sentences were drawn randomly (please see Wichmann et al. 2018 for more details).

Sentence segmentation was the first step where the extracted text corpus is split into sentences so as to facilitate the extraction of entities with a sentence tokeniser tool.

Entity extraction involved the detection of entities using Named Entity Recognition (NER) using spaCy, Flair and the Stanford CoreNLP NER taggers.

Labelling involved the creation of training data for the classifier to detect supply–buy relationships. Only sentences with two or more detected organisational named entities were admitted to the labelling process where Amazon MTurkers annotated supply–buy relations through a web app (for details of the labelling process, including Cohen's Kappa, see Wichmann et al. 2018). The extracted dataset includes 3887 aerospace news articles sentences and 8231 labelled relationships between entities. Example sentences are given in Table 4.

Classification is the step where a machine learning model is trained to classify relations between extracted entities. Differing from Wichmann et al. (2018), who used BiLSTM, we opted for a pretrained Bidirectional Encoder Representations from Transformers (BERT) from Huggingface and performed transfer learning following (Brintrup 2023), who reported superior results.

Knowledge graph representation. Once each potential link between any two firms is classified as existing or not-existing, then, a knowledge graph can then be
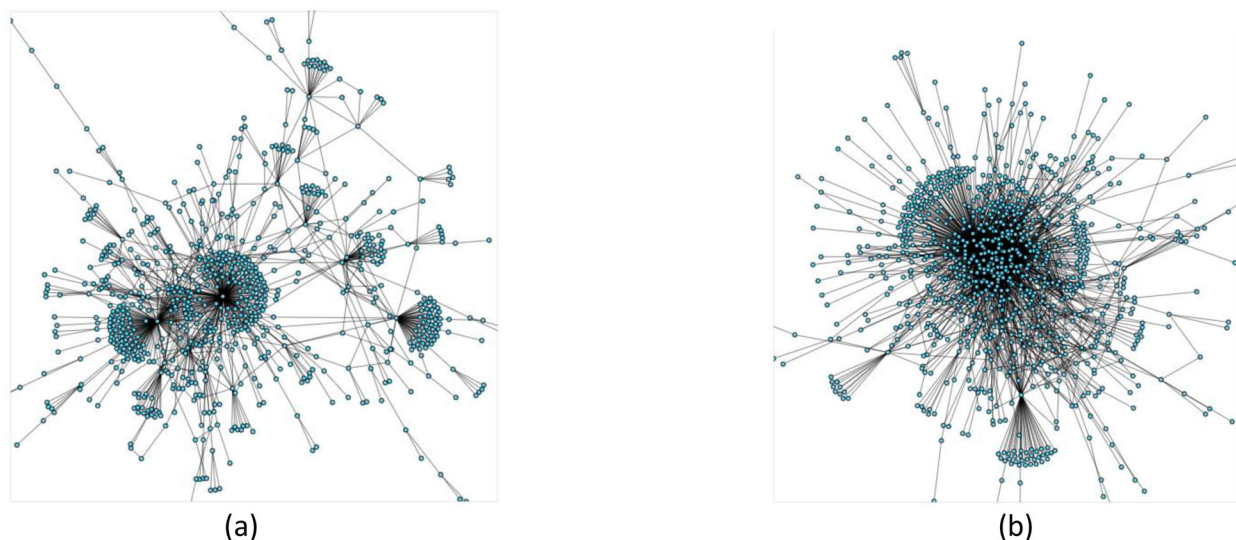
Figure 3. (a) Knowledge Graph before link prediction and (b) Knowledge graph after link prediction.

Table 4. Example sentences extracted from Reuters text corpus.

The Boeing Co. selected UTC Aerospace Systems to work with it to develop advanced actuation technology for the U.S. Air Force.

Hexcel will extend its partnership with Airbus Helicopters by supplying composite materials for the new H160 helicopter.

In 2014, RUAG and Tata Group signed an agreement for the latter to become a key supplier of the program

Advanced composite manufacturer, Teledyne CML Composites is celebrating the award by GKN Aerospace of a package of composite nacelle parts

Boeing Co has entered into a $1-billion agreement with Russian titanium producer VSMPO-Avisma Corp., to source various titanium products from 2011 through 2015

used to codify relations amongst the entities resulting in a graph with 1009 company nodes and 1177 supply–buyer relationships (Figure 3a).

Link prediction. Next, Graph Neural Networks (GNN) were used to identify hidden links in the network based on Kosasih and Brintrup (2021b). The GNN is trained on a subset of the known links, and the resulting classifier is used to predict any potential link presence in other pairs of nodes. The application of GNN resulted in the identification of 1200 more links, leading to a graph with 1009 company nodes and 2377 supply–buyer relationships (Figure 3b), increasing graph density from 0.0023 to 0.0046.

Let us now analyse some of the additional links that have been predicted. There are 18 links predicted to have a relationship with the Boeing Company PLC, which include a number of airlines, electronics and battery producers, raw materials suppliers.

Several observations can be made. First, the model predicted links between Boeing and various airlines (SAS, Cathay, Viva Air, Emirates Airline, China Southern Airlines, Aegean Airlines, Saudi Arabian Airlines and JAL). This is most likely because our input news source

contain information about connections between these airlines and Airbus, another competitor who topologically is in a similar role with Boeing. This is interesting as there is indeed a link between these companies and Boeing, however, clearly, the direction of these links is incorrect as Boeing is a supplier to these airlines, and is not a buyer. This, however, is a known limitation of the GNN approach that we use (Kosasih and Brintrup 2021a), which is an open area of research.

The second limitation we have identified is the dynamically changing nature of the links which our model cannot capture. For instance, Aegean Airlines currently buys from Airbus, although it has had a buy relationship with Boeing in that past.[1] This points to the need for research on the accuracy of supply chain dependency information, for example via time-based uncertainty metrics, periodic data re-extraction and model retraining, or a combination of all of these. Although there is technology available to capture and store dynamically changing information, what generally is problematic in supply chains is that a breakage of previous links are typically not reported. They may be inferred, for example if we know that a new contract has been signed with a different provider for the same product, although such inference would be far from generalisable and certain. Another issue is determining an appropriate period which link prediction algorithms are retrained. In some instances, the algorithm should not forget previous information, whilst in others it should, as a relationship has been replaced. These are currently open questions in the field of knowledge graph research.

The third challenge that arises from our analysis is a lack of ground truth for verification. We identify several electronics and battery producers, who are predicted to

supply to Boeing but are not able to verify these relationships. From previous studies, accuracy estimates ranged between 80% and 90% accuracy (see Kosasih and Brintrup 2021a; Brintrup et al. 2018) where a number of links, whose existence were a priori known, had been masked during the training/testing phase. In real life, links that are predicted may not be easily verifiable, with little opportunity to retrain the algorithm, unless the company deploying the algorithm takes active steps in continuously correcting and sourcing training data. Thus these unverifiable predictions would point to useful starting points for investigation, should such relationships were to be deemed important by the inquirer. It would be useful to estimate uncertainty of resulting links that are predicted, such that the inquirer can be guided to prioritise high certainty predictions. The impact of false positives depends on how DSCS results are used. For example, in the illustrative use case 3 in Section 3, the wrong location had been flagged as a potential dependency, whereas in the use case 6 potentially confidential information had revealed. Before acting on these, companies need to ensure results are verified.

Systemic Risk Evaluation. Here, we use topologically based systemic risk measures to identify critical nodes in the aerospace network, using approaches proposed by Ledwoch et al. (2018) and Brintrup et al. (2018). Four measures were used: degree centrality, eigenvector centrality, betweenness centrality and closeness centrality.

Degree centrality is the count of number of relationships of a firm, which relate to 'the extent with which a firm has an impact on operational decisions or strategic behaviour of other firms' (Kim et al. 2011). Table 5 shows the top 10 companies that score highly before and after prediction. Whilst focal firms such as Boeing and Airbus are kept, after link prediction the list becomes more aerospace focussed, and therefore captures systemically important firms to the industry including Honeywell, which produces aircraft engines and other parts, Thales, which provides avionics, Rockwell Collins, providing avionics and information technologys products.

Eigenvector centrality measures node importance based on the importance of its neighbours. Hence disruptions in companies with high eigenvector centrality would impact other important nodes in the network, leading to cascade effects. Here we see Rolls-Royce as a high ranking supplier both before and after link prediction with addition of companies such as Thales and Lockheed Martin (Table 6).

Betweenness centrality measures how often a node appears on the shortest, connector paths. Nodes with high betweenness centrality control the flow of materials and communication, and thus can control the speed

Table 5. Degree centrality before and after link prediction.

Before		After	
Company	Degree Centrality	Company	Degree Centrality
Boeing	0.221	Boeing	0.521
Airbus	0.147	Airbus	0.336
Toyota	0.063	Toyota	0.063
GM	0.023	Rolls-Royce	0.053
Rolls-Royce	0.023	Honeywell	0.041
Apple	0.023	Thales	0.037
BMW	0.023	Rockwell Collins	0.033
GKN Aerospace	0.019	Lockheed Martin	0.028
Embraer	0.016	GKN Aerospace	0.027
Rockwell Collins	0.014	GM	0.027

Table 6. Eigenvector centrality before and after link prediction.

Before		After	
Company	Eigenvector Centrality	Company	Eigenvector Centrality
Boeing	0.594	Boeing	0.510
Airbus	0.366	Airbus	0.398
Rolls-Royce	0.095	Rolls-Royce	0.109
Rockwell Collins	0.085	Honeywell	0.090
UTC Aerospace Systems	0.079	Thales	0.080
BAE Systems	0.076	Rockwell Collins	0.080
Alcoa	0.074	Lockheed Martin	0.027
GKN	0.072	Mitsubishi Motors Corp	0.068
Spirit AeroSystems	0.072	Chrysler	0.067
FACC	0.071	Bombardier	0.064

Table 7. Betweenness centrality before and after link prediction.

Before		After	
Company	Betweenness Centrality	Company	Betweenness Centrality
Boeing	0.337	Boeing	0.643
Airbus	0.226	Airbus	0.234
Toyota	0.111	Toyota	0.075
BMW	0.054	Apple	0.025
Kobe Steel	0.045	Kaiser	0.021
Alcoa	0.043	General Motors	0.019
Apple	0.038	GKN Aerospace	0.018
GM	0.037	Pratt & Whitney	0.016
General Motors	0.035	BMW	0.015
GKN	0.034	Foxconn	0.015

with which information and material can be disseminated in the network and may act as bottlenecks. Here we observed companies from other sectors playing an important role in aerospace industry – possibly through common suppliers in raw materials and electronics components, with addition of companies such as Apple, Kaiser, Pratt and Whitney, Foxconn. This would highlight the inter-dependence between these sectors to the insurer and the possibility of risk transfer (Table 7).

Table 8. Closeness centrality before and after link prediction.

Before		After	
Company	Closeness Centrality	Company	Closeness Centrality
Boeing	0.340	Boeing	0.593
Airbus	0.322	Airbus	0.510
Kobe Steel	0.279	Rolls-Royce	0.404
GKN	0.278	Kobe Steel	0.402
Bridgestone	0.276	Tenneco	0.400
ASCO	0.275	Thales	0.399
Hexcel	0.274	Rockwell Collins	0.399
Alcoa	0.273	Yazaki	0.398
Eaton Corporation	0.267	GM	0.398

Closeness centrality is the inverse of the mean distance from a node to other nodes and measures how close a firm is to other firms in the network. Firms with high closeness benefit from short supply chains and suffer less from classical supply chain issues such as bullwhip effect, as well as gaining the ability to act independently, given its ability to access information in the network faster than other firms (Kim et al. 2011). From a risk perspective though, Brintrup et al. (2018) has interpreted the measure as how fast in one node disturbances would disseminate, should buffers do not prevent cascades. After link prediction, we see the addition of companies such as Rolls-Royce, Tenneco, Thales, Rockwell Collins, Yazaki and GM as critical companies (Table 8).

Overall, both degree and eigenvector centrality shows Rolls Royce, Honeywell and Thales to be critical suppliers to the aerospace industry based on the DSCS example in our case study. Betweenness centrality gives additional information on possibly risk transfer between industries. A company that is embedded within the aerospace ecosystem could make use of these results by keeping a close watch over these critical companies as it is likely that disruptions on them will impact the ecosystem's function. Similarly, the insurer may wish to consider these interdependencies before underwriting risks involved.

In summary, we observe that DSCS facilitates the aggregation of supply data encompassing multiple supply chains and industries, which, without DCSC would have involved the insurer to manually obtain information from multiple parties. Overlapping supplier base between multiple firm and industries become evident once data extraction and aggregation is automated. Link prediction provides additional information that the insurer can act upon. However, our analysis also highlights several technical limitations. For example, in terms of obtaining news articles, the choice of keywords used to search for articles and the source of data will produce bias. We have seen that link directionality is problematic with GNN. Additional data extraction such as products produced, locations could not only help with the directionality problem but also give a better picture of risk. Entity resolution

remains an open problem as many companies are identified as different entities, even though they are related through parent companies. In terms of link prediction, methods to reduce search space of checking node pairs for potential link existence are needed. Uncertainty modelling should be explored as a confidence intervals would help guide the inquirer. This would also necessitate topological measures that could handle links with uncertainty. Whilst the challenges we identified here are specific to the visibility and risk challenge identified in Table 1 (Challenge E) and solved by a set of specific methods proposed in the literature, it is worth noting that bias, uncertainty, explainability are likely to be common challenges brought upon by the use of AI in DSCS.

6. Synthesis, conclusion and managerial implications

In this paper, we conceptualized the emerging practice of '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. While the 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 analyse data become available, providing an important opportunity to help organizations fill information gaps in their supply chain.

A mixed methods approach enabled us to explore how DSCS is proposed in the literature (Section 2), what risks are involved (Section 3), the level of uptake in industry (Section 4). An in-depth quantitative case study helped us explore what new knowledge can DSCS generate, as well as technical limitations (Section 5).

DSCS offers significant promise in a wide range of impactful areas in supply chains, offering complimentary solutions to tackle hard problems such as end-to-end supply chain visibility. A review of existing literature mapped the extant DSCS surveillance challenges that have been proposed by researchers and industrialists showing a number of diverse areas of interest ranging from predicting sustainability scores to supplier performance. A number of commercial offerings were also reviewed, highlighting a growing number of start-up companies offering services in this area, mainly in areas of supply chain visibility, supply chain sustainability and ESG scoring, and prediction of financial health. While the literature review showed diverse areas of application, commercial offerings generally are more focussed on visibility. Similarly, while the literature review showed a diversity of AI methods and data sources, commercial

offerings were mainly focussed on NLP approaches to obtain web based data.

From a technical standpoint, much research needs to be undertaken. 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. It is also important to highlight that not while DSCS could be helpful towards completing some of the gaps in the surveillar's knowledge, it is highly likely information obtained via DSCS will not be fully complete, and will contain uncertainties. Thus research into data integration, imbalance, interpretability and uncertainty quantification remain important issues for the technical advancement of DSCS.

The increased power of large language models (LLM) provides an opportunity for DSCS. For example, Transformer neural network we used in our case study surpassed performances reported earlier. The utilisation of chatbots based on LLM (such as ChatGPT4) is another interesting avenue for future research. Using these one could convert natural language queries into queries that can be answered using graph based data, which most of the reported DSCS mechanisms have been based on so far (e.g. Kosasih 23, Wichmann 21). For instance, instead of querying 'Which companies have the highest betweenness centrality?' (which might be too technically specific for general supply chain manager), ChatGPT might be able to support general query such as 'Which companies have the highest risk?' and provide a summary based on different types of measures.

Overall, our survey results showed that: certain types of surveillance challenges such as ethical supplier practice, sustainability and innovation are prioritised more than others. There is a clear distinction between the manufacturing sector who were more likely to rate predictions of Delays, Excess capacity, Quality issues and Price offers whereas the services sector preferred sustainability and ethical practice. However improved visibility underpins many of these challenges.

We found that most companies are using their internal data and manual searches, with only a few companies buying DSCS as a service. Increased supply chain size, complexity and lack of visibility may drive the use of DSCS, especially DSCS that is AI powered. On the other hand, the literature shows key data sources that are emerging for DSCS include publicly available or subscription datasets such as carbon emission reporting, financial records, World Wide Web. These currently remain untapped. While several private companies claim to gather DSCS, their underlying datasets and algorithms are not transparent, which may yield potential risks to practitioners. Important future research direction we foresee is transparency in DSCS, and also trade-offs between investments into DSCS practice and datasets, and return on investment.

Algorithm performance was generally rated higher than explainability in all surveillance challenges; however, the importance of explainability differed significantly, between different surveillance challenges. For example, manufacturers overwhelmingly preferred explanability in the prediction of supplier performance, but preferred accuracy in demand forecasting. Respondents raised questions on the authenticity of data and concerns over accuracy of predictions made by AI enabled DSCS.

We subsequently illustrated how DSC could be applied to extract risk insights from the aerospace sector, by combining a number of proposed algorithmic approaches in the literature. Our results showed that whilst accuracy might reach 80–90% on identified supplier–buyer dependencies, uncertainty and lack of verifiability pose limitations.

The concerns raised by our case study and the surveyed manufacturers present important questions in adopting DSCS. Digitalising 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. Outsourcing DSCS could obscure data sources and algorithmic logic used to derive conclusions. Thus organizations that want to pursue DSCS 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, errors and question the authenticity of predictions. In tandem, explainable AI practices should be explored so that algorithmic decisions can be back traced, and otherwise posthoc interpreted.

As DSCS, and AI in supply chain management in general, present previously unobtainable information, thought needs to be put into how this will be safely incorporated into supply chain processes, weighing uncertainties of predictions, against cost of obtaining such information and defining appropriately balanced actions. It is important to note that DSCS does not prescribe action, but supports evidence towards action, and taking appropriate and balanced action on the intelligence provided remains within the surveillar's responsibility.

While DSCS shows much potential to aid supply chain risk management, the loss of data control by organisations, especially with datasets that are combined through multiple proprietary resources, and may change jurisdictions, present significant challenges to trustworthiness for DSCS and organisations that undertake it. More research on legal frameworks needs to be carried out to support policy making.

Note

1. https://en.about.aegeanair.com/company/history/milestones/ and https://www.planespotters.net/airline/Aegean-Airlines

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

Data availability statement

Due to the nature of the research, supporting data is not available.

Notes on contributors

Alexandra Brintrup is a professor in digital manufacturing and is leading the Supply Chain Artificial Intelligence Lab at the University of Cambridge She is a fellow of Darwin College and she is the Digital Manufacturing Theme leader at the Alan Turing Institute. Alexandra obtained her PhD in artificial intelligence from Cranfield University. She then worked at the ABN AMRO Bank as a quantitative analyst. She was later appointed as research fellow at the Complex Agent Based Dynamic Networks (CAB-DyN) research centre at the University of Oxford, where she studied supply chains from a complex networks perspective. She joined Cambridge in 2016. Her research interests include complex adaptive systems, complex networks, AI and machine learning in supply chain management.

Edward Kosasih is a PhD student in the Supply Chain AI Lab at the University of Cambridge. His research interests include machine learning, network science and operations research. He is currently working with Dr Alexandra Brintrup and Aviva Quantum on a supply chain risk modelling project using algorithms from graph theory and machine learning. Edward has previously been affiliated with Keysight Technologies, Delft University of Technology and A∗STAR Singapore. He received his Bachelor degree in electrical engineering at the National University of Singapore.

Ge Zheng is a research associate in the Supply Chain AI Lab at the University of Cambridge at the Institute for Manufacturing (IfM), Department of Engineering, University of Cambridge. Her current research focusses on machine learning in supply chains. Before moving to Cambridge, Ge did her PhD in the Department of Computing and Informatics at Bournemouth University on urban transport networks using deep learning technologies. Her interested areas include predictive systems for supply chain operations, pattern recognition and/or classification, intelligent transportation systems and healthcare applications.

Philipp Schaffer is a visiting student at the University of Cambridge, Department of Engineering. His research focuses machine learning in supply chain mapping. He is in the final year of his master's degree in Business Administration and Mechanical Engineering at RWTH Aachen University. Philipp holds a Bachelor's degree in business administration and mechanical engineering and gained practical industry and consulting experience in the field of procurement and supply chain management.

Güven Demirel is a reader in Supply Chain Management at Queen Mary University of London. He holds a PhD in Physics from the Max Planck Institute for the Physics of Complex Systems, Dresden, Germany and he worked as a research fellow at the Nottingham University Business School, University of Nottingham and Lecturer in Logistics and Supply Chain Management at the Essex Business School, University of Essex before joining QMUL.

Bart L. MacCarthy has been a professor of Operations Management at the University of Nottingham since January 2003. After an early career in industry, he undertook his PhD at the University of Bradford in the early 1980s, followed by postdoctoral work in the Mathematics Institute at Oxford University. Professor MacCarthy has conducted extensive research in supply chain management, particularly in the areas of supply chain planning, scheduling and control using modelling, analysis and simulation techniques. His current research interests are in how digitalisation is affecting the nature of contemporary supply chains, their configuration, management and control.

ORCID

Alexandra Brintrup http://orcid.org/0000-0002-4189-2434
Edward Kosasih http://orcid.org/0000-0001-5293-2641

References

Ahmadi, B., B. Javidi, and S. Shahbazmohamadi. 2018. "Automated Detection of Counterfeit ICs Using Machine Learning." *Microelectronics Reliability* 88–90: 371–377. https://doi.org/10.1016/j.microrel.2018.06.083

Ahn, Y. Y., S. E. Ahnert, J. P. Bagrow, and A.-L. Barabási. 2011. "Flavor Network and the Principles of Food Pairing." *Scientific Reports* 1 (1): 196. https://doi.org/10.1038/srep00196

Alikhani, R., S. A. Torabi, and N. Altay. 2019. "Strategic Supplier Selection Under Sustainability and Risk Criteria." *International Journal of Production Economics* 208: 69–82. https://doi.org/10.1016/j.ijpe.2018.11.018

Aristodemou, L., and F. Tietze. 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. https://doi.org/10.1016/j.wpi.2018.07.002

Astill, J., R. A. Dara, M. Campbell, J. M. Farber, E. D. G. Fraser, S. Sharif, and R. Y. Yada. 2019. "Transparency in Food Supply Chains: A Review of Enabling Technology Solutions." *Trends in Food Science & Technology* 91: 240–247. https://doi.org/10.1016/j.tifs.2019.07.024

Azadnia, A. H., M. Z. M. Saman, and K. Y. Wong. 2015. "Sustainable Supplier Selection and Order Lot-Sizing: An Integrated Multi-Objective Decision-Making Process." *International Journal of Production Research* 53 (2): 383–408. https://doi.org/10.1080/00207543.2014.935827

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

Barratt, M., and A. Oke. 2007. "Antecedents of Supply Chain Visibility in Retail Supply Chains: A Resource-Based Theory Perspective." *Journal of Operations Management* 25 (6): 1217–1233.

Baryannis, G., S. Dani, and G. Antoniou. 2019. "Predicting Supply Chain Risks Using Machine Learning: The Trade-off Between Performance and Interpretability." *Future Generation Computer Systems* 101: 993–1004. https://doi.org/10.1016/j.future.2019.07.059

Basole, Rahul C., and Marcus A. Bellamy. 2014. "Supply Network Structure, Visibility, and Risk Diffusion: A Computational Approach." *Decision Sciences* 45 (4): 753–789. https://doi.org/10.1111/deci.12099

Blackhurst, J. V., K. P. Scheibe, and D. J. Johnson. 2008. *Supplier risk assessment and monitoring for the automotive industry. International journal of physical distribution and logistics management* 38 (2): 143–165.

Blackhurst, J., T. Wu, and P. O'Grady. 2004. "Network-based Approach to Modelling Uncertainty in a Supply Chain." *International Journal of Production Research* 42 (8): 1639–1658. https://doi.org/10.1080/0020754030360001646064

Boateng, F. O., J. Amoah-Mensah, M. Anokye, L. Osei, and P. Dzebre. 2017. "Modeling of Tomato Prices in Ashanti Region, Ghana, Using Seasonal Autoregressive Integrated Moving Average Model." *Journal of Advances in Mathematics and Computer Science*: 1–13.

Bode, C., and S. M. Wagner. 2015. "Structural Drivers of Upstream Supply Chain Complexity and the Frequency of Supply Chain Disruptions." *Journal of Operations Management* 36 (1): 215–228. https://doi.org/10.1016/j.jom.2014.12.004

Brennen, A. 2020. "What Do People Really Want When They Say They Want 'Explainable AI?' We Asked 60 Stakeholders." In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–7. Association for Computing Machinery. https://doi.org/10.1145/3334480.3383047

Brintrup, A. 2023. "Understanding Complex Supply Networks: An Interdisciplinary Journey." *NetSci 2023*, July, Vienna.

Brintrup, A., J. Pak, D. Ratiney, T. Pearce, P. Wichmann, P. Woodall, and D. Mcfarlane. 2020. "Supply Chain Data Analytics for Predicting Supplier Disruptions: A Case Study in Complex Asset Manufacturing." *International Journal of Production Research* 58 (11): 3330–3341. http://dx.doi.org/10.1080/00207543.2019.1685705

Brintrup, A., P. Wichmann, P. Woodall, D. Mcfarlane, E. Nicks, and W. Krechel. 2018. *Predicting Hidden Links in Supply Networks*. Complexity; Hindawi. https://doi.org/10.1155/2018/9104387

Brintrup, A., E. E. Kosasih, B. L. MacCarthy, and G. Demirel. 2022. "Digital Supply Chain Surveillance: Concepts, Challenges, and Frameworks." In *The Digital Supply Chain*, 379–396. Elsevier.

Brockmann, N., E. Elson Kosasih, and A. Brintrup. 2022. "Supply Chain Link Prediction on Uncertain Knowledge Graph." *ACM SIGKDD Explorations Newsletter* 24 (2): 124–130. https://doi.org/10.1145/3575637.3575655

Cannas, V. G., M. P. Ciano, M. Saltalamacchia, and R. Secchi. 2023. "Artificial Intelligence in Supply Chain and Operations Management: A Multiple Case Study Research." *International Journal of Production Research*, 1–28. https://doi.org/10.1080/00207543.2023.2232050

Chiou, C. Y., C. W. Hsu, and W. Y. Hwang. 2008. "Comparative Investigation on Green Supplier Selection of the American, Japanese and Taiwanese Electronics Industry in China." *IEEE International Conference on Industrial Engineering and Engineering Management*: 1909–1914. https://doi.org/10.1109/IEEM.2008.4738204

Christopher, M., and H. Peck. 2004. "The Five Principles of Supply Chain Resilience." *Logistics Europe* 12 (1): 16–21.

Clarke, R. 2019. "Risks Inherent in the Digital Surveillance Economy: A Research Agenda." *Journal of Information Technology* 34 (1): 59–80. https://doi.org/10.1177/0268396218815559

Dachowicz, A., S. C. Chaduvula, M. Atallah, and J. H. Panchal. 2017. "Microstructure-Based Counterfeit Detection in Metal Part Manufacturing." *JOM* 69 (11): 2390–2396.

Devlin, J., M. W. Chang, K. Lee, and K. Toutanova. 2018. Bert: Pre-training of Deep Bidirectional Transformers for Language Understanding. arXiv preprint:1810.04805.

Dohale, V., M. Akarte, A. Gunasekaran, and P. Verma. 2022. "Exploring the Role of Artificial Intelligence in Building Production Resilience: Learnings from the COVID-19 Pandemic." *International Journal of Production Research*, 1–17. https://doi.org/10.1080/00207543.2022.2127961

Dolgui, A., and D. Ivanov. 2023. "Metaverse Supply Chain and Operations Management." *International Journal of Production Research*, 1–13. https://doi.org/10.1080/00207543.2023.2240900.

EY, Ernst and Young. 2020. https://www.ey.com/en_gl/consulting/covid-19-why-real-time-visibility-is-a-game-changer-for-supply-chains.

Falkheimer, J., and M. Heide. 2015. "Trust and Brand Recovery Campaigns in Crisis: Findus Nordic and the Horsemeat Scandal." *International Journal of Strategic Communication* 9 (2): 134–147.

Graham, S., and D. Wood. 2003. "Digitizing Surveillance: Categorization, Space, Inequality." *Critical Social Policy*. https://doi.org/10.1177/0261018303023002006

Harland, C., R. Brenchley, and H. Walker. 2003. "Risk in Supply Networks." *Journal of Purchasing and Supply Management* 9 (2): 51–62. https://doi.org/10.1016/S1478-4092(03)00004-9

He, M., H. Ji, Q. Wang, C. Ren, R. M. Lougee, H. Ji, Q. Wang, C. Ren, and R. Lougee. 2014. "Big Data Fueled Process Management of Supply Risks: Sensing, Prediction, Evaluation

and Mitigation." *Proceedings of the 2014 Winter Simulation Conference* : 1005–1013.

Ho, W., T. Zheng, H. Yildiz, and S. Talluri. 2015. "Supply Chain Risk Management: A Literature Review." *International Journal of Production Research* 53 (16): 5031–5069. https://doi.org/10.1080/00207543.2015.1030467

Ivanov, D., A. Dolgui, and B. Sokolov. 2019. "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.

Ivanov, D., A. Dolgui, B. Sokolov, and M. Ivanova. 2017. "Literature Review on Disruption Recovery in the Supply Chain." *International Journal of Production Research* 55 (20): 6158–6174. https://doi.org/10.1080/00207543.2017.1330 572.

Jiao, J. R., X. You, and A. Kumar. 2006. "An Agent-Based Framework for Collaborative Negotiation in the Global Manufacturing Supply Chain Network." *Robotics and Computer-Integrated Manufacturing* 22 (3): 239–255. https://doi.org/10.1016/j.rcim.2005.04.003

Jüttner, U., H. Peck, and M. Christopher. 2003. "Supply Chain Risk Management: Outlining an Agenda for Future Research." *International Journal of Logistics: research and applications* 6 (4): 197–210.

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

Kinra, A., D. Ivanov, A. Das, and A. Dolgui. 2020. "Ripple Effect Quantification by Supplier Risk Exposure Assessment." *International Journal of Production Research* 58 (18): 5559–5578. https://doi.org/10.1080/00207543.2019.1675 919

Klassen, R. D., and A. Vereecke. 2012. "Social Issues in Supply Chains: Capabilities Link Responsibility, Risk (Opportunity), and Performance." *International Journal of Production Economics* 140 (1): 103–115. https://doi.org/10.1016/j.ijpe. 2012.01.021

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

Kosasih, E. E., and A. Brintrup. 2021b. *Reinforcement Learning Provides a Flexible Approach for Realistic Supply Chain Safety Stock Optimisation*. ArXiv:2107.00913 [Cs]. http://arxiv.org/abs/2107.00913

Kuo, R. J., Y. C. Wang, and F. C. Tien. 2010. "Integration of Artificial Neural Network and MADA Methods for Green Supplier Selection." *Journal of Cleaner Production* 18 (12): 1161–1170. https://doi.org/10.1016/j.jclepro.2010.03.020

Ledwoch, A., A. Brintrup, J. Mehnen, and A. Tiwari. 2018. "Systemic Risk Assessment in Complex Supply Networks." *IEEE Systems Journal* 12 (2): 1826–1837. https://doi.org/10.1109/JSYST.2016.2596999

Lee, B. 2021. "Price Prediction for Supply Chain Order Assignment." MEng Dissertation, University of Cambridge

Lianos, M., and M. Douglas. 2000. "Dangerization and the End of Deviance: The Institutional Environment." *The British Journal of Criminology* 40 (2): 261–278. https://doi.org/10.1093/bjc/40.2.261

Lin, Y., and L. Zhou. 2011. "The Impacts of Product Design Changes on Supply Chain Risk: A Case Study." *International Journal of Physical Distribution and Logistics Management* 41 (2): 162–186.

MacCarthy, B. L., W. A. Ahmed, and G. Demirel. 2022. "Mapping the Supply Chain: Why, What and how?" *International Journal of Production Economics* 250: 108688. https://doi.org/10.1016/j.ijpe.2022.108688

Manuj, I., and J. T. Mentzer. 2008. "Global Supply Chain Risk Management." *Journal of Business Logistics* 29 (1): 133–155. https://doi.org/10.1002/j.2158-1592.2008.tb00072.x

Martínez, A., J. Nin, E. Tomás, and A. Rubio. 2019. "Graph Convolutional Networks on Customer/Supplier Graph Data to Improve Default Prediction." In *Complex Networks X*, edited by S. P. Cornelius, C. Granell Martorell, J. Gómez-Gardeñes, and B. Gonçalves, 135–146. Springer International Publishing. https://doi.org/10.1007/978-3-030-144 59-3_11

Murdoch, B. 2021. "Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a new era." *BMC Medical Ethics* 22 (1): 122. https://doi.org/10.1186/s12910-021-00687-3

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

ONS, Office for National Statistics. 2022. https://datascienceca mpus.ons.gov.uk/using-natural-language-processing-for-the -analysis-of-global-supply-chains/.

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

Psarommatis, F., G. May, P.-A. Dreyfus, and D. Kiritsis. 2020. "Zero Defect Manufacturing: State-of-the-art Review, Shortcomings and Future Directions in Research." *International Journal of Production Research* 58 (1): 1–17. https://doi.org/10.1080/00207543.2019.1605228

Russell, S., and P. Norvig. 2009. *Artificial Intelligence: A Modern Approach*. Prentice Hall.

Samvedi, A., V. Jain, and F. T. Chan. 2013. "Quantifying Risks in a Supply Chain through Integration of Fuzzy AHP and Fuzzy TOPSIS." *International Journal of Production Research* 51 (8): 2433–2442.

Sharma, Ajit. 2023. "Artificial Intelligence for Sense Making in Survival Supply Chains." *International Journal of Production Research*, 1–24.

Swartz, P. G., H. S. K. King, T. G. Garnett, J. R. Psota, and Inc Panjiva. 2019. System, Method, and Apparatus for Determining and Correcting Shipping Volumes. U.S. Patent Application 16/159,584.

Tang, O., and S. Nurmaya Musa. 2011. "Identifying Risk Issues and Research Advancements in Supply Chain Risk Management." *International Journal of Production Economics* 133 (1): 25–34. https://doi.org/10.1016/j.ijpe.2010.06.013

Tang, C., and B. Tomlin. 2008. "The Power of Flexibility for Mitigating Supply Chain Risks." *International Journal of Production Economics* 116 (1): 12–27.

Trautrims, A., B. L. Maccarthy, and C. Okade. 2017. "Building an Innovation-Based Supplier Portfolio: The Use of Patent Analysis in Strategic Supplier Selection in the Automotive Sector." *International Journal of Production Economics* 194: 228–236. https://doi.org/10.1016/j.ijpe.2017.05.008

Tummala, R., and T. Schoenherr. 2011. "Assessing and Managing Risks Using the Supply Chain Risk Management Process (SCRMP)." *An International Journal* 16 (6): 474–483.

Wang, X., P. Tiwari, and X. Chen. 2017. "Communicating Supply Chain Risks and Mitigation Strategies: A Comprehensive Framework." *Production Planning & Control* 28 (13): 1023–1036. https://doi.org/10.1080/09537287.2017.1329562.

Wichmann, P., A. Brintrup, S. Baker, P. Woodall, and D. McFarlane. 2018. "Towards Automatically Generating Supply Chain Maps from Natural Language Text." *IFAC-PapersOnLine* 51 (11): 1726–1731. https://doi.org/10.1016/j.ifacol.2018.08.207

Wolf, T., L. Debut, V. Sanh, J. Chaumond, C. Delangue, A. Moi, P. Cistac, et al. 2020, October. "Transformers: State-of-the-Art Natural Language Processing." Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations (pp. 38–45).

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

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

Ye, S., Z. Xiao, and G. Zhu. 2015. "Identification of Supply Chain Disruptions with Economic Performance of Firms using Multicategory Support Vector Machines." *International Journal of Production Research* 53 (10): 3086–3103.

Zage, D., K. Glass, and R. Colbaugh. 2013. "Improving Supply Chain Security Using Big Data." *IEEE International Conference on Intelligence and Security Informatics*: 254–259. https://doi.org/10.1109/ISI.2013.6578830

Zheng, G., L. Kong, and A. Brintrup. 2023. "Federated Machine Learning for Privacy Preserving, Collective Supply Chain Risk Prediction." *International Journal of Production Research*, 1–18. https://doi.org/10.1080/00207543.2022.2164628