Investigation of Supply Chain Risk Utilising Cynefin Model

Yang Chu
Manchester Business School,
The University of Manchester, Booth Street West, Manchester, UK, M15 6PB
Email: yang.chu@mbs.ac.uk

Abstract: Supply chains seem increasingly susceptible to unexpected disruptions. The concept of supply chain (SC) risk still remains ambiguous [44] and a lack of understanding of supply chain disruption makes its identification, categorisation and measurement more difficult. There are qualitative differences among risks and important non-quantifiable information cannot be ignored. Biased assessment could be generated if models, tools and techniques are misleadingly implemented. Moreover, development of methods for risk assessment without considering the attribute of the risk could lead to assessment failure. In the light of these gaps, the purpose of the study is to utilise the Cynefin model to help managers further understand both quantitative and qualitative aspects of supply chain disruptions to avoid biased assessment. More specifically, it attempts to provide a framework for analysing the attributes of supply chain disruption to assist decision making on the methods for its assessment.

Keywords: Supply Chain, Risk, Cynefin Model

I. Introduction

The challenge of managing of SC disruptions is becoming increasingly important among organisations. Recent survey evidence found that 72% of procurement executives feel that the vulnerability of their SCs has increased over the past 24 months [46]. However, perhaps most alarming is organisational readiness to deal with the disruption. The same survey shows that less than 20% of procurement executives believe that they are well prepared to manage their SC risks. SC disruptions can have a significant financial and operational impact on organisations not properly prepared [21].

Risk can be assessed through methods that are either quantitative, qualitative or a mixture of the two. Quantitative methods attempt to examine absolute value ranges often with probability distributions for the business outcome and consequently, involve more sophisticated analysis [38]. For example, models such as real options approach [14], decision tree model [70], and frequency space method [7] etc, are designed to quantitatively assess supply chain risks. In contrast, qualitative methods compare the relative significance of risks facing a business in terms of its probability and impact, often based on experience description and scales [38]. For instance, an AHP-based tool in assessing its enumeration of risks was developed [67]. The AHP technique was also applied to assess 17 typical supply chain risks [49]. Meanwhile, a multi-criteria scoring procedure was developed to assess supplier specific risk indices [6].

While these advances have been extremely valuable to our understanding of risks within supply chain structures, there is the potential for misapplication. Different types of risks should be analysed differently based on its attributes. The attributes of a risk include drivers, probability and consequence of the risk occurring. Understanding risk attributes is important because it affects the decision on approaches for risk assessment. There is a trend that statistical and risk modelling techniques in areas where sufficient data can be collected is employed to assess risks [65]. For instance, the cause and impact of an internal quality risk can be clearly established. Statistical process control can be applied to detect if processes deviate from quality specifications.

However, not every risk can be quantified and trying to quantify some risk that naturally cannot be quantified may waste time and resources. Drivers of some risks such as a terrorist attack are often interacted with each other and the relationship between cause and impact is sometimes difficult to clearly establish. Such attributes determine that methods for assessing such risks should be more qualitative rather than quantitative. If the causes of risk are so complex that no reliable data can be obtained, then statistics can no longer be used [65].

The complexity of a risk makes its assessment difficult. Quantifiable and non-quantifiable data associated with the attribute of a risk needs to be carefully analsyed before risk assessment is conducted. In this study the author is interested in how the attribute of a risk affects the choices of methods for its assessment. The motivation is that despite a great deal of research that has been conducted in the realm of Supply Chain Risk Management (SCRM), little attempt has been made to develop a method for analysing a supply chain risk in assisting decision making on methods for its assessment. The author proposes that one method of addressing this gap is to look at risk utilising the Cynefin model.

The Cynefin model provides a taxonomy that guides certain explanations and/or solutions that may be applied to a problem. The model can be potentially applied to categorise supply chain risks for the purpose of its assessment. The succinct taxonomy based on the Cynefin model could help academicians and practitioners further understand the nature of a supply chain disruption and develop appropriate methods for its assessment.

In application of the Cynefin model to analyse the attributes of a risk, a series of propositions are derived.

Proposition 1 Internal risks are more likely to be quantified than SC network risk and environmental risk

Proposition 2 Accuracy of assessment of a risk from a SC network can be improved if both quantitative and qualitative methods are applied.

Proposition 3 Quantitative tools are more accurate in assessing internal risk than environment risk

Proposition 4 An event without order and patterns is uncertain and unlikely to be assessed in a structured way.

II. Supply Chain Disruptions

What is SC risk? Both academician and practitioners are still struggling to understand it. In spite of more than 19 SC risk definitions i.e. [2] [12] [18] [13] [24] [29] [31] [56] [58] [66] [72] [73] etc. found in literature, the basic concept of SC risk, like the concept of risk, has not prevailed over such definitional issues. Different terms such as SC disruption and vulnerability have been used to describe SC risk. SC vulnerability is defined as the existence of random disturbances that cause deviations in SC components and materials from expected schedules, all of which cause negative impacts on the involved organisations in a SC [56]. SC risk is defined as risk in SC centers around the disruption of "flows" related to information, materials, products and money between organisations [29]. SC risk is also defined as unplanned and unanticipated events that disrupt the normal flow of goods and materials within a SC [2] [25] [32].

There are common elements in many of these definitions and most authors include "disruptions of flows such as information, materials, products, and cash" in their SC risk definitions i.e. [12] [13] [28] [66] [31] [18]. Unfortunately, the evidence from literature demonstrates that it is less likely to have a universal definition of SC risk which can be applied to every industry sector. Given the mixed use and interpretation of terminologies, the definitional issue of SC risk remains to be clarified.

III. Supply Chain Risk Classification

There are more than 50 ways to classify SC disruption in the literature, but none of these classifications are mutually exclusive. This indicates that the SC disruption is not a simple issue. The drivers of a disruption are interacted with each other and the relationship between causes and effects are sometimes difficult to clearly established, which makes risk assessment much more difficult.

The author develops a risk classification by combing the classification proposed by Chopra and Sodhi [13] with the classification developed by Juttner et al [28]. The generic risk assessment framework contains nine original risk categories: disruptions, delays, systems, forecast, IP, procurement, receivables, inventory and capacity [13]. Disruptions can be caused by a pandemic, national disaster, supplier bankruptcy, piracy, war and terrorism. Another eight categories above cover risk sources related to day to day operations. However, many authors i.e. [40] [58] etc found that operational risk can cause SC disruption therefore, it is necessary to expand Chopra and Sodhi's categories to address the operational risk.

One point that is especially interesting here is that SC risks do not simply arise from within an organisation but from its SC network and environment also. For example, labour disruption or quality issues could arise in the focal company but could also arise from its supplier, however, the impact does not necessarily have to be on the organisation where the risk occurs. This reflects the key characteristic of SC risks: any risk that occurs in one organisation could have an impact on other affected parties simultaneously. This is a critical point and determines the complexity of a SC disruption. Therefore, SC risk is further classified as internal related, network related and environmentally related risk [28] as shown in Table 1.

Environmental risk arises from the supply chain–environment interaction such as natural disaster, soci-political actions, lawsuit and accidents. Network-related risk sources arise from interactions between firms within the SC such as raw material procurement risk, raw material availability and energy shortage etc. Internal risk sources arise from within an organisation such as labour strikes, production problems and management problems etc. Various ways of categorising sources of SC risks indicates that SC risks are complex and various sources could lead to SC disruptions.

IV. Sense-making Framework for Supply Chain Risk Assessment

The Cynefin model was developed by David Snowden and his collaborators at the IBM Institute of Knowledge Management in 2002. Cynefin is a Welsh word and translated means 'habitat' [52]. Its meaning includes cultural and social as well as environmental perspectives [17]. It is a framework employed to describe problems, situations and systems. The framework provides a taxonomy that guides certain explanations and/or solutions that may be applied to a problem. Initial application of the Cynefin model is in the field of organisational knowledge management, cultural change and community dynamics [52]; subsequently, it is expanded into product development, market creation, branding, decision-making, strategy, national security and policy making. It initially has four domains known, knowable, complex and chaotic [52] and Snowden added disorder as fifth domain later, as shown in Figure 1.

Table 1 Supply Chain Risk Classification

Risks	Sub risks	I[1]	N[2]	E[3]
Disruptions Disaster	Natural disasters including earthquake, fire flood, storm, monsoon, blizzard, drought, heat wave, tornado, hurricane, typhoon, tsunami, epidemic, famine, avalanche			X
	Non-natural disaster including explosion, shipwreck, crash, fire and contamination etc		X	X
	War, terrorism, piracy			X
	Pandemic			X
	Financial: supplier financial instability, loan availability, supplier bankruptcy, restructuring business		X	
	Economic including; economic crisis, inflation, access to funds			X
	Labour disruption, e.g., labour disputes , strikes and protests	X	X	
	Lack of resources, e.g., labor availability, skilled labour and facility availability	X	X	
	Dependency on a single source of supply a the capacity and responsiveness of alternative suppliers ,		X	
	Energy risk including shortage of energy, high price of energy and Power shortage			X
	Political issues such as; corruption, fiscal, regulatory. Trade embargos, riot, revolution, civil commotion, protest, legal, policy (Political & Governmental & Regulatory)			X
	Environmental including; pollution and climate change			X
	Competition		X	
Delay	High capacity utilisation at supply source		X	
	Inflexibility of supply source		X	
	Poor quality or yield at supply source including supplier inability to meet quality standards		X	
	Excessive handling due to border crossings or change in transportation modes		X	
	Logistics: number of brokers, transfer points, vessel capacity and channel overload, port issues and infrastructure,		X	
Systems	Information infrastructure breakdown (Hardware failure), Software failure	X	X	
	System integration or extensive systems networking		X	
	E commerce	X	X	
	Ability to share information with supplier	X		
	IT Attack	X	X	
	Communication (management security)	X	X	
Forecast	Inaccurate forecasts due to long lead times, seasonality, product variety, short life cycles, small customers base	X		
	Bullwhip effect or information distortion due to sales promotions, incentives, lack of supply-chain visibility and exaggeration of demand in times of product shortage		X	
	Lead time variance	X	X	
Legal and IP	Vertical integration of supply chain (Law/rule breach)		X	
	Global outsourcing and markets		X	
	Contractual problem: Long-term versus short-term contracts, malicious act, contract management	X	X	
	Change in legislation			X
	Fraud	X	X	
Procurement	Exchange rate fluctuation			X
	Percentage of a key component or raw material procured from a single source		X	
	Industry wide capacity utilisation		X	
	Raw material price		X	X
Receivables	Number of customers, change in demand		X	
	Financial strength of customers		X	
	Product price		X	X
Inventory	Rate of product obsolescence	X	X	
	Inventory holding cost	X	X	
	Product value	X	X	
	Demand and supply uncertainty such as demand-supply mismatch		X	
	Inaccurate delivery	X	X	
Capacity	Cost of capacity	X	X	
	Capacity flexibility , Capacity shortage	X	X	
Operation	Failure in core operations, misapplication of rules, assumptions, systems and procedures,	X	X	
	Technical failure	X	X	
	Change in technology	X	X	

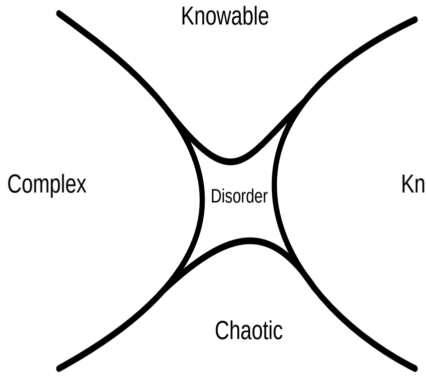

Figure 1: Cynefin Model [52]

"Known" issues are generally ordered, clear, simple and the relationship between cause and effect is repeatable. This is the domain of scientific inquiry [17] [52], in other words issues in this domain can be evaluated with sufficient scientific data. The consequences of any response can be predicted with great certainty [16].

"Knowable" issues are generally ordered but complicated. Cause and effect of an issue are separated over space and/or time in this domain but can be perceived and forecasted after gathering and further analysing data. This is the domain of scientific knowledge [5] [17] [52].

"Complex" issues are unordered and cause and effect can only be perceived in retrospect and situations involve many interacting causes and effects. This is in the domain of social systems [17]. There are no precise quantitative methods to forecast its behaviors [16].

[1] Internal
[2] Network
[3] Environmental

"Chaotic" issues are unordered, beyond our experience and cause and effect at systems level are not discernable [52].

"Disorder" issues are difficult to recognise and there is no way of knowing about what type of cause-effect exists. The way out of this domain is to break down the issues into constituent parts and assign each of these to one of the other four domains [52].

Since SC disruptions may arise from various sources, risks associated with SC may not simply concentrate on one domain but disperse in different domains of the model. Important, non-quantifiable information cannot be ignored since there are qualitative differences among some risks. Strategic SCRM process should incorporate dynamic realities of complex SC risk nature. It appears that many SC risks still remain too complex to make coherent decisions on how to best manage them. SC managers may make inappropriate decisions on the selection of assessment models due to lack of understanding the nature of a disruption. Some SC risks are too undefined to be assessed. Trying to quantity some complex risks which naturally cannot be quantified may waste time and resources. The application of the Cynefin model shows that a particular risk can be analysed in a structured way to determine the type of methods for its assessment.

V. Risk Assessment Method

Quantitative analysis is usually based on mathematical formulas whereas qualitative assessment is based on experience description and scales.

Both quantitative and qualitative techniques have been used in assessing SC risk. List of techniques and models for SC risk identification and its analysis have been appeared in SC risk literature and are shown in table 2 and table 3. However, some other general risk assessment techniques including Delphi method, Event Tree Analysis (ETA), Fault Tree Analysis (FTA) and questionnaire have not been popularly appeared in the SC risk literature.

Table 2 SC Risk Identification Techniques and Models

Risk Identification techniques and models	References
Value focused process engineering (VFPE)	[42]
Ericsson Risk Management Evaluation tool (ERMET)	[43]
Cause-effect diagrams	[18]
A HAZOP-Based Approach	[2]
Checklist	[2]
Stress test	[11]
Failure modes and effects analysis (FMEA)	[61]
Brainstorming	[50]

Table 3 SC Risk Analysis Techniques and Models

Risk analysis techniques and models	References
Bayesian network	[46]
Fragility factor index (threat level (cost) and impact (fragility, potential disruption)	[55]
Analytical Hierarchy Process (AHP)	[19], [67]
Conceptual framework for analysis of vulnerability (qualitatively)	[56]
Supply chain mapping	[18]
ABC analysis	[63]
Mutil-level framework for risk analysis	[45]
Risk-Matrix	[62]

Proposition 1: Internal risks are more likely to be quantified than network risk and environmental risk

The more frequently a risk occurs, the more likely the risk can be quantitatively evaluated. Risks which can be assessed based on the reliable scientific data are grouped in the 'known' domain where methods for assessing such risks can be guided by standards of "best-practice", rationality and scientific knowledge [5] [52] [68]. Such risks can be responded with predefined procedures. For example, from a focal company point of view, internal quality risk is technology related [70], internal controllable [67] and micro risk [35]. Statistical process control can detect if processes deviate from quality specifications [71]. Probability and loss of defect product/component can be easily modeled based on historical data within an organisation. Internal risks are likely fall into the 'known' domain such as quality risk, inventory risk, operational risk and capacity related risk as shown in table 4, 5 and 6. Risk mitigation actions to the impacts of these risks can be predicted with confidence. Sensing data, categorising it and a course of action can be taken immediately in this domain.

Table 4 Factors that Contribute to Capacity Risk

Factors that contribute to capacity risk	References and prior research
Design changes	[40][54][71][70] [74]
Product complexity	[70]
Transportation	[3][54][70]
Delay of materials	[11] [26] [70]

Table 5 Factors that Contribute to Inventory Risk

Factors that contribute to inventory risk	References and prior research
Demand and supply uncertainty	[11] [15]
Product value	[11]
Inventory holding cost	[11] [15]
Rate of product obsolescence	[11]
Theft	[15]
Inaccurate delivery	[15]

Therefore, quantitative methods play an important role in assessing risk from the internal organisation. However, the proposition does not mean that this type of risk should not be assessed by qualitative methods, especially the risk from its network. For example, risks such as quality risk can arise from both internal or/and network. This leads on to the second proposition

Table 6: Factors That Contribute to Operational Risk

Factors that contribute to operational risk		References and prior research
Process related	Failure in core operations	[40]
	Manufacturing capacity constraints	[4] [40][51]
	Process variations in yields, equipment and utilitisation	[23] [40]
	Changes in technology/ emergence of a disruptive technology	[4] [23] [40]
	Changes in operating exposure	[40]
	Property losses	[4]
	Component/material shortages	[4]
	Logistic errors	[4] [23][57]
	Storage/warehouse operation problems	[4] [23]
	Budget overrun	[4]
	Communication/IT disruptions	[4]
	Manufacturability	[74]
Misapplication of rules, assumptions, systems and procedures	Forecast errors	[4] [23]
	Inventory control failure	[23]
	Inadequate scheduling methods	[23]
	Financial control failure	[23]
	Contract terms	[4]
	Failure to comply with regulatory environment	[23]
	Information control failure	[9] [23] [41]

Proposition 2: Accuracy of assessment of a risk from supply chain network can be improved if both quantitative and qualitative methods are applied.

In the ‘knowable’ domain, probability, cause and consequence of a risk exist and are stable, but there is need for sufficient scientific analysis or expert opinions to support its assessment. Network related risks such as demand risk, quality risk from a supplier and demand risk as shown in table 7 and 8 are grouped in the ‘knowable’ domain. Risks here are complicated. First of all, the reliability of secondary data from external organisations may be low; secondly, the amount of information that a focal company can obtain from its suppliers and/or customers is limited. If the causes are so complex that no reliable data can be obtained and statistics can no longer be used; then some qualitative information has to be obtained in order to get a comprehensive perspective of an issue.

However, if sufficient time and resources are given, causes, consequences and probability of a risk in this domain can be discovered and ascertained exactly. For example, demand risk is complicated but can be decomposed into different factors as shown in table 7. Methods can be developed to understand the linkages between cause and consequence of such risk occurring. For example, season factor can be treated as an important factor to predict the fluctuation of the demand and relevant data can be acquired. However, change in consumer tastes cannot be mathematically modeled. The prediction for such risk is more accurate if both qualitative and quantitative methods are applied. Although the cause and consequence of such risks are separated in space and time, risks in this domain can be systematically assessed over time and locations with a certain degree of accuracy [68].

Table 7: Factors That Contribute to Demand Risk

Factors that contribute to change in demand risk	References and prior research
Market changes	[3] [30]
Inaccurate demand forecast	[11] [22]
Changing consumer tastes	[59]
Fluctuation of demand	[22] [57] [58] [71]
Supplier’s inability to manufacture at required speed	[54]
Economic crisis	[22]
Delay in material flows	[11]
Variance in the volume and assortment desired by the customer	[40] [37]
Delayed/inappropriate new product introductions	[64] [27] [40]
Distorted information from the downstream supply chain members	[40]

Table 8: Factors from Supply Chain Network That Contribute to Quality Risk

Factors that contribute to network related quality risk	References and prior research
Lack of control the quality of product/service provided by suppliers	[44]
Differing quality cultures and norms in the member firms	[54]
Failure of supplier to maintain capital equipment	[41][54][71] [74]
lack of supplier training in quality principles and techniques	[41][54][71] [73]
Damage that occurs in transit	[41][54][71] [73]
Suppliers inability to meet quality standards	[41][59] [73]
Not availability of specific skills required to the suppliers	[14]

Proposition 3 Quantitative tools are more accurate in assessing internal risk rather than environment risk

Data from the internal organisation is much more accessible and reliable than data from external organisations. When stochastic models are applied, the possible values with a probability distribution have to be defined to each uncertain variable. It is difficult to make right assumptions if external data is unavailable or unreliable. Similarly when a deterministic model is applied, techniques such as stress test and sensitivity analysis require high reliability of the data. Risks from SC’s environment are difficult to be quantitatively assessed due to a lack of reliable data. The author argues that some environmental risks such as political issues, economic crisis and pandemic are very complex and should be grouped into the ‘complex’ domain.

Issues in the ‘complex’ domain continually evolve in unpredictable, interactive and uncontrollable patterns [5]. Issues in this domain are ‘open problems’ which can never be fully solved [5]. Risk assessment is possible, however there are no sufficient scientific supports such as precise models in understanding for predicting the probability, causes and consequences of a risk. Possible consequences can only be known after a risk has occurred. Knowledge is at best qualitative due to too many potential interactions to disentangle specific causes and effects in this domain [17]. Analysis should be broader with less emphasis on details. Due to a lack of past experience and knowledge in recognising these risks, the causes and consequences of an event is only coherent in retrospect. Swine Flu disease in 2009 is a typical example. Due to the complexity of such a virus, many countries' governments initially had limited information about the virus and therefore failed to predict the degree of its impacts on the economy. The SCRM methods/tools work efficiently in managing risks in the 'known' and 'knowable' domains but not in the 'complex' domain. Some typical risks in the complex domain are normally from environmental sources such as disaster, technological risk and political risk as shown in Table 9, 10 and 11.

Table 9 Sources of Environmental Risk

Disaster sources		**References**
Nature disasters	Fire, thunderstorm, flood, monsoon, blizzard, storm, drought, heat wave, tornado, hurricane, typhoon, earthquake, tsunami, epidemic, famine, avalanche	[1][69][34] [3][49][6] [4]
Economic crisis	Shifts in wage rates, interest rate, exchange rates, and prices	[35][40]
War & terrorism		[1][18][6]
Illness/Pandemic	Such as foot-mouth disease, swine flu, bird flu	

Table 10: Factors That Contribute to Technological Risk

Factors that contribute to technological risk	**References and prior research**
Technological evolution	[8] [14][20][48] [60]
Low ability to adopt the new technologies	[14] [54][71]
Emergence of a disruptive technology	[4]
Sharing of quality technology	[59]
Access to technology	[59]
New technology	[59]
Technology gaps existing in potential suppliers	[70]
Technical complexity	[20] [36]
Complexity of product	[20] [36]
Incompatible information systems	[11] [41]
Inflexibility of supply chain technology	[1]
Lacking technical innovation	[41] [71] [72]

Table 11: Factors That Contribute to Political Risk

Factors contribute to political risk	**References**
Political environment	[33]
Geopolitical instability	[1]
Legal, regulations	[4][6]
Governmental incentives	[4]
Restrictions or commitments relating to the use of the material, product, or service	[74]
Government policy	[74]

Proposition 4 An event without order and patterns is uncertain and is unlikely to be assessed in a structured way.

Uncertainty is defined as the situation when it is not possible to attach a probability to the likelihood of an event occurring [38]. Risk is concerned with situations in which probabilities can be attached to particular events occurring, whereas uncertainty defines situations in which probabilities cannot be attached [10]. It exists in situations where decision-makers lack complete knowledge, information or understanding of possible consequences. The author argues that uncertainty should fall in the 'chaotic' domain.

In the 'chaotic' domain, issues are described as unordered, beyond our experience. SC disruptions in the 'chaotic' domain have no order and no patterns. They are generally new and no one can know how to react it in a structured way, until the event happens. When such events happen, initially organisations would react in an uncontrollable and unpredictable way. Previous risk assumptions can be disrupted and knowledge can be precipitated when such events happen. For example, the eruption of a volcano in Iceland which caused massive disruption of air transportation in the UK in April 2010, is typical example. All planes from the UK were simply grounded for several days. It is not usually useful to spend significant time and a large amount of resource trying to describe why events in the 'chaotic' domain unfolded in certain way [68]. Events in this space require crisis management and need to be actively managed [52]. The relationship between cause and effect in this domain are impossible to determine because they shift constantly and no manageable patterns exist [53]. Searching for right answers would be meaningless in a chaotic context.

VI. Conclusions and future work

The paper demonstrates a method for analysing SC risk for the purpose of its assessment, utilising the Cynefin model. The Cynefin model indicates that risks factors in different domains should be identified, assessed, mitigated and monitored by different methods. Understanding SC risk differences in known, knowable, complex and chaotic domains is important in the development and implementation of risk assessment methods. A list of risks that are reviewed and analysed through the Cynefin Model will benefit practitioners and scholars in the development and implementation of their risk assessment tools, models and techniques. Additionally, the SC risk taxonomy constructed in this paper is useful for SCRM practitioners in seeking to understand disruption factors.

There are several indications to SCRM from the Cynefin model:

1. The senses-making Cynefin Model indicates that risks in different domains should be identified, assessed, mitigated and monitored by different methods. Probability and consequences of some SC risks that cannot be completely understood by quantitative methods such as mathematic modeling should be assessed using qualitative methods such as expert opinions. For example, it is wasting time to quantify the probability of an economic crisis whereas it is worth quantifying its impact on a specific SC. Some methods such as AHP or HAZOP-based approach perhaps, can assess risks in the 'known' and 'knowable' domains, whereas brainstorming, Delphi study and questionnaires can

be applied to identify risks in the chaotic and complex areas. This explains the phenomena that there are various methods developed for SCRM in literature but none of them individually can assess all types of risks. Therefore, methods should be applied based on the nature of risks.

2. SC risk taxonomy gives practitioners and scholars a clear structure regarding current research state of SC risk. This taxonomy is developed based on authors' best knowledge from current literature. With increasing development of technology, experiences and knowledge some risks possibly move around within the four domains e.g. demand risk may move from 'knowable' domain to 'known' domain. Due to the complexity of the nature of the risk, author keeps this taxonomy open. Two individuals could argue that the same risk belongs in different domains, based on their personal experiences and expertise.

3. Understanding SC risk differences in known, knowable, complex and chaotic domains is important in the development of methods to assess SC risk.

The proposed method in this paper is a first step in the development of methodologies to improve the accuracy of SC risk assessment. As such, future research should concentrate on the following two issues: first of all, the SC risk taxonomy needs to be further defined and expended. Secondly, existing tools, models and techniques for assessing SC risk could be further validated by the application of the Cynefin Model.

Acknowledge:

The Author wishes to acknowledge the support of the Engineering and Physical Sciences Research Council (EPSRC) The author also thanks Qun Wang for her kind assistance in researching and preparing this paper.

References:

Please contact the author to get the reference lists

Background of the Author

Dr. Yang Chu is a graduate of the School of Mechanical, Aerospace and Civil Engineering at the University of Manchester and a research consultant with Oriel Group Practice, specialising in the areas of project finance and risk and financial modelling. He is currently working as a postdoctoral research associate on an EPSRC project: Managing Supply Chain Vulnerability: Understanding the Impact of Supply Chain Design' at Manchester Business School at The University of Manchester.