Control Structures in supply chains as a way to manage unpredictable cyber-risks

Sepúlveda Estay, Daniel Alberto; Khan, Omera

Publication date:
2016

Document Version
Peer reviewed version

Control structures in supply chains as a way to manage unpredictable cyber-risks

Daniel A. Sepulveda Estay (dasep@dtu.dk)
Management Engineering, Technical University of Denmark

Omera Khan
Product Operations Management, Aalborg University

Summary Abstract

Supply chain growth, and their dependence on Information Technology (IT), is making cyber risks an increasingly unmanageable threat through traditional risk assessment methods. Systemic analysis methods have been identified as alternatives to traditional methods. This paper analyzes the application of a systemic risk analysis methodology to understand cyber risks in the supply chain. A generic supply chain is analyzed, and information flows, dynamic structures and the influence of cyber-attack on these are identified. This paper argues that a systemic approach is more efficient in detecting vulnerabilities, enabling an evolving disruption response process and culture in the supply chain.

Keywords: Cyber-risks, Supply Chain Management, Resilience

Introduction

In recent years, supply chains have increasingly grown in complexity, coupled by their dependence on Information Technology (IT), in becoming what has been defined as cyber-physical systems, or the embedding of IT in applications in the real world (Gollmann et al., 2016). Although this complexity has allowed a faster operation and frontier-less communication, it has also exposed supply chains to new vulnerabilities (Manuj et al., 2008) because of the increased number of nodes and connections present in the cyber supply chain (Dederick et al., 2008). Disruptions resulting from these vulnerabilities have been placed at US 300 billion in losses and, not surprisingly, cyber-attacks have been identified as one of the most important risks in the supply chain (WEF, 2013).

Cyber risks in the supply chain, i.e., those risks associated with the use of IT, differ substantially from other supply chain risks that may be present. Some of these differences are summarized in Table 1, including aspects such as physical location, complexity limitation, and anonymity.

Table 1: Cyber versus Physical Risks in the Supply Chain

Physical Supply Chain (Flow of goods)	**Cyber Supply Chain (Flow of Information)**
Physical location is relevant	Physical location is irrelevant
Anonymity is uncommon	Anonymity is common
Limited complexity	Unlimited complexity
Buffers are useful	Buffers are risky
Mainly components risk	Mainly interaction risks

Companies have been managing risks in their supply chains through causal chain analysis techniques, primarily with a focus on its physical dimension, such as Failure Tree Analysis (FTA), Failure modes and criticality analysis (FMECA), or through probabilistic methods. For systems with limited complexity and mainly focused on component performance, these techniques have been useful.

However, two main issues stand out. First, with the increase in supply chain complexity, these techniques are increasingly onerous to implement and maintain. In order to consider all potential modes of failure, important resources are required to create these traditional risk analyses or to maintain them as existing risks change or new ones appear. Second, Supply chain IT development has allowed both a decrease in the individual supply chain component failure, as well as an increase in the number of interaction failures in the supply chain.

This means that a supply chain can fail even if all its components worked as expected, as the risk is materialized in the interaction between these components, situation that would be invisible to traditional methods, centered on component reliability and direct contributing factors to the specific risk. This is rendering traditional risk methods increasingly inadequate for the complex systems in which they need to be used. The following table summarizes some of the reasons why traditional approaches are insufficient for the modern supply chain.

Table 2: Traditional way versus their insufficiency

Traditional way	**Reason for insufficiency**
Focus is on structure-to-risk	Nothing is said about reaction-to-risk
Focus is on components	Nothing is said about the interaction between these components
Prepares organization for specific risks	Organization needs to react to any risk
Human effects are centered around operator error	Human effects can lead to risk even if no operator error is made
Assumes a constant structure	Structure is changing continuously

A first aspect for inquiry is exposed at this point, regarding other tools that might exist to deal with these insufficiencies. This paper proposes additional approaches that may complement traditional analyses, and which might bridge the insufficiencies listed above addressing not only preparation for cyber-risks, but also reaction to cyber risks, i.e., cyber-resilience.

Additional to causal chain and probabilistic analyses, a third approach has been proposed in literature to understand risk, namely systemic risk analysis. This approach seeks to change the problem management from one of individual component reliability (i.e., each part of the supply chain functions as it is supposed to do), to a control problem of the complete relevant

supply system. Techniques such as the Systems Theoretic Accident Model & Processes (STAMP) have been used areas such as product development, and manufacturing operations, and its advantages and outcomes have been well documented for these cases (Altabbakh et al., 2014). However, systemic methods of analysis have been used to analyze supply chains only in a limited way. A second aspect of inquiry is thus the way in which systemic analyses of cyber risks, allow us to better understand and manage these risks in supply chains.

Cyber resilience in supply chains

According to Christopher and Peck, supply chain resilience is the ability of a supply chain to return to its original state or move to a new, more desirable state after being disturbed (Christopher et al., 2004). Supply chain resilience has thus evolved as an additional concept to supply chain risk. While risk management entails the examination of all possible outcomes of a process, weighing the potential returns against the potential risks of investment, resilience management characterizes organizational reaction to low probability / high impact events and unforeseeable disruptions to create competitive advantage (Petit et al., 2010).

Literature has taken different perspectives to examine supply disruptions and resilience in supply chains, such as conceptual (Christopher et al., 2004), behavioral (Ellis et al, 2010), qualitative (Sheffi et al, 2005; Craighead et al, 2007), simulation/modelling (Wu et al., 2007; Nair et al., 2011), and network structure (Kim et al., 2015). Such a variety of approaches has enabled a number of different ways in which to understand the phenomenon, yet has also led to a degree of confusion about the level of analysis appropriate for different situations.

All the approaches to supply chain resilience are static except for Sheffi and Rice's proposal (Sheffi et al., 2005), which consisted of the application to supply chains of a disruption theory for production systems developed in Norway (Absbjornslett, 1999), proposing what was defined by them as the "disruption profile". This approach is identified as dynamic since the response of the supply chain changes over time, and is qualitatively described through eight distinct phases of evolution, i.e., preparation, disruptive event, first response, initial impact, time of full impact, preparation for recovery, recovery, and long-term impact (Sheffi et al., 2005). However, none of the definitions of resilience found in our literature review has considered system control as part of their definition.

The other approaches to supply chain resilience describe the supply chain at a specific point in time, and are thus static in nature, akin to taking a picture of the current state of the supply chain resilience. Moreover, many of the definitions present in literature, such as Tang (Tang, 2006) or Longo & Oren (Longo & Oren, 2008), limit their contribution only to proposing a definition for resilience, without the subsequent suggestion of any qualitative description, or quantitative measure of this supply chain resilience.

Starting from Sheffi & Rice's approach, Khan and her team have proposed that the length and depth of the disruption can be considered as a direct indicator of the resilience of a process, as can be seen in Figure 1. If a process has a longer disruption in its performance and/or a performance disruption is greater, then it can be said to have a lower/weaker resilience (Khan et al., 2015).

Although these measures might make sense for simple systems, it is not clear if they will have similar effects to complex interconnected supply networks. For example, Kim and his team have already suggested that redundancy might hinder resilience for some supply network configurations (Kim et al., 2014). It has also been mentioned that redundancy can be effective systems consisting of purely electromechanical components. However, when

there is software involved as well as the interaction of human operators, redundancy can sometimes contribute to accidents through, e.g., design complexity (Leveson, 2011).

Systemic risk analysis methods.

The use of feedback loops for a systemic understanding of risk in industrial systems including the human component is not new. In 1998, the analysis of industries with high levels of hazard (Carroll, 1998), suggested that traditional solutions, although well-intentioned, fail to help through their unintended side-effects, as illustrated in the Figure 1.

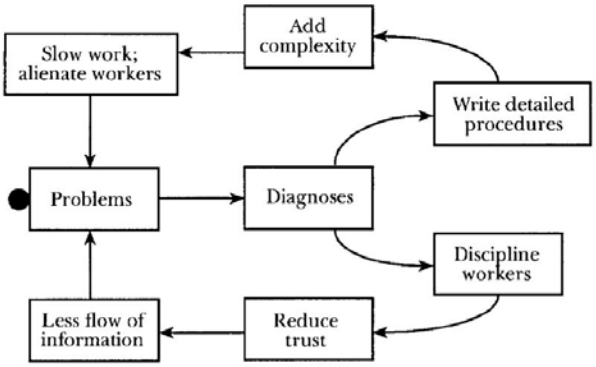

Figure 1: Common mitigation measures and their side effects (Carroll 1998)

Kang and his team have used a systems approach to identify Limiting Conditions for Operation (LCOs in operations, extensible to supply chains (Kang et al., 2005). Their approach acknowledges three important aspects: 1) a system dynamics approach ensures a causal relationship in the establishment of the feedback loop structure, 2) the approach is useful for understanding the behavior of a complex system over time, and 3) a systemic approach is useful in conceptualizing a thorough understanding of human interactions within complex systems.

More recently, Gahdge et al., (2013) proposed a systemic approach based on the three pillars of risk identification, risk assessment and risk mitigation. Through the generation of a system dynamics model containing different attributes and parameters, risks can be simulated and sensitivity analyses can be obtained on the relevance of each parameter. However, although the results and simulation clearly point out to a system dynamics model, it is unclear what feedback loops, delays and sources of inertia, i.e., stocks (Sterman, 2000) were considered.

Garbolino et al. (2016) and his team used system dynamics modeling and risk analysis to propose a dynamic risk analysis method that includes both approaches. They acknowledge that this modelling approach focuses on the strengthening of constraints, and it allows a dynamic process where industrial systems continually adapt to external and internal changes to achieve their goals. They propose a ten-step approach that results in scenario analysis through a model. It is however restricted to a single plant and its internal process, thereby lacking the integration with other supply partners.

Our research process did not find documented literature on the application of systemic risk analysis methods to supply chains.

Research Hypothesis

This paper considers three main hypotheses that direct the choice and application of different frameworks for understanding cyber-risks in the supply chain.

First, supply chains have structures that determine how they react over time to disruptions such as cyber-attacks. According to the System Dynamics approach, an observed behavior in a supply system is the result of an underlying structure (Forrester, 1961; Sterman, 2000). In a supply chain, these cause either the flow of physical goods (e.g., raw materials, physical products, and physical services) or a flow of information (e.g., Purchase Orders, Money, Coordination emails, digital products or services).

Second, physical flow of goods is controlled by the information flow around that process. The physical flow follows the instructions laid down by the information flow in the supply chain. Closed loop control structures involve feedback loops (Doyle et al., 1992), and it is expected the same thing will happen for the case of supply chains.

Third, cyber-attacks to a supply chain will necessarily affect its information flows, and involve one or more feedback loops, which are then later reflected as an operational disruption.

Methodology

The process that was followed for the analysis of a supply chain through a systemic risk analysis follows the STAMP model (Systems-theoretic Accident Model and Processes) as proposed by Leveson (2011). This paper does not explain the methodology, rather focuses on the results and consequences of its application to cyber risks in the supply chain.

This is a model based on systems theory rather than traditional analytic reduction and reliability theory. A safe operation is seen as an emergent property resulting from the interactions of the components with each other and the environment. The problem of avoiding "accidents" (unplanned loss events) thus becomes a dynamic control problem. Figure 3 shows a control system representation of a controlled process. Only an extract of the analysis is shown.

Results

Control systems representation

Let us consider a simple supply chain as a single-level transaction between a buyer and a seller, for the ownership of a product.

This single-level supply chain already involves at least three members, i.e., buyer, seller, transporter, also known as "agents" (Swaminathan et al., 1998). Through such a process, a buyer will inform a seller that it wants to buy an item from them. The seller agrees, and contacts a transportation agent to move the product from the seller to the buyer. The representation of such a supply chain is a reflection of the information gathered on how such a supply chain is working, and is by definition, incomplete (Sterman, 2002). The information flow present in this simple supply chain is not linear and it requires many flows of information, between the different agents involved, as represented in Table 3.

Table 3 Information Flows in generic 1-level supply chain

Information Flow Number	Description	Emiting agent	Receiving Agent	Required Predecesor
IFL1	Purchase Order (P.O.)	Buyer	Seller	-
IFL2	P.O. Confirmation	Seller	Buyer	IFL1
IFL3	Service Order (S.O.)	Seller	Transporter	IFL2
IFL4	S.O. Confirmation	Transporter	Seller	IFL3
IFL5	Pickup Coordination	Transporter	Seller	IFL4
IFL6	Delivery Coordination	Transporter	Buyer	IFL4
IFL7	Transport Documentation	Transporter	Seller	IFL4
IFL8	Transport Documentation	Seller	Buyer	IFL2
IFL9	S.O. Payment	Seller	Transporter	IFL7
IFL10	S.O. Payment Confirmation	Transporter	Seller	IFL9
IFL11	P.O. Payment	Buyer	Seller	IFL8
IFL12	P.O. Payment Confirmation	Seller	Buyer	IFL11

As it can be seen, these information flows are not isolated and in themselves may require a specific flow predecessor to take place. For example, in order that IFL-2 can happen (Purchase Order Confirmation) from the seller to the buyer, a previous purchase order information flow must have been emitted by the buyer to the seller, i.e., IFL-1. These create feedback loops, which can be identified in the following control loop diagram in Figure 2. The loops involved are mentioned in Table 4.

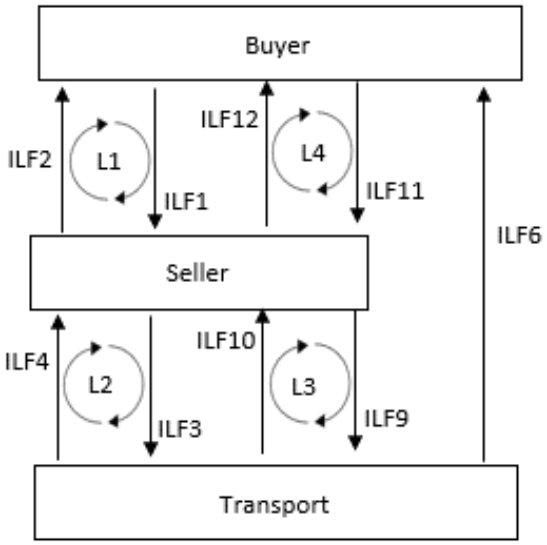

Figure 2: Basic information supply chain (partial representation of flows).

Table 4 Information Feedback Loops for a single-level supply chain

Control Loop	Description	Information Flows (IFL) involved
L1	Purchase Order Loop	IFl1 - IFL2
L2	Service Order Loop	IFL3 - IFL4
L3	S.O. Payment Loop	IFL9 - IFL10
L4	P.O. Payment Loop	IFL11-IFL12

Table 5: Analysis if unsafe control actions from a cyber-attack (Extract)

UCA	Desc.	Type 1	Type 2	Type 3	Type 4
UCA #1	Send Service Order to Transport Agent	Seller does not send service order to transport agent, when there has been a confirmed purchase order Transport agent does not receive the service order sent by the seller.	Seller sends service order confirmation to buyer with the wrong product specification. Buyer receives the purchase order confirmation with the wrong product specification. Seller sends purchase order confirmation considering inaccurate stock information.	Seller sends service order to transport agent too late to arrange a timely pickup/delivery	not applicable (Service Order is either sent or not)
UCA #2	Send Purchase Order confirmation to buyer	Seller does not send the purchase order confirmation to buyer when there has been a purchase order received. Buyer does not receive the purchase order confirmation sent by the seller	Seller sends purchase order confirmation to buyer with the wrong product specification. Buyer receives the purchase order confirmation with the wrong product specification. Seller sends purchase order confirmation considering inaccurate stock information.	Seller sends the purchase order confirmation to buyer before identifying existing stock.	Not applicable (Purchase Order Confirmation is either sent or not)
UCA #3	Send service order confirmation	Transport Agent does not send the service order confirmation to the seller when there has been a service order received The seller does not receive a service order confirmation, when it has issued a service order to the transport agent.	Transport agent sends service order confirmation with wrong specifications which are then later confirmed with buyer	Transport agent send service order confirmation to seller too late to make timely pickup arrangements	Not applicable (Service Order Confirmation is either sent or not)

Hazard Analysis

For a generic, single-tier supply chain, the accidents and unacceptable losses in the case of cyber-attacks to supply chains have to be defined. This is highly dependent on the specific supply chain, and in the case of a generic supply chain example, a few examples are mentioned in the following table.

Table 6: Unacceptable accidents in the supply chain (extract)

Accidents	**Description**
A1	No product is delivered to customer due to cyber-attack
A2	Wrong product is delivered to customer due to a cyber attack

The system as defined has different control actions, for the hazards that can be identified. These can have four types of dangers. (Leveson, 2011). Type 1: The control action is present, thus causing an unsafe conditions; Type 2: The control action is absent, thus causing an unsafe condition; Type 3: The control action was applied to early or too late, thus causing an unsafe condition, and Type 4: The control action was applied to little or too much, thus causing an unsafe condition.

An extract of the type of analysis that can be achieved for a generic supply chain, starting from each Unsafe Control Action (UCA) is shown in the following Table 5.

Discussion

This paper proposes a detailed and concise way of representing the flow of information/communication for a simplified, generic supply chain. This representation was based on the identification of the relevant supply system, the agents interacting in the supply system, the communication paths, and the resulting feedback loops. Control structures were identified in the supply chain as a result, based on the communication flows present.

The example presented in this paper is not intended to be an exhaustive analysis of a supply, but rather sought to show the application of a systemic risk analysis technique to the case of cyber risks in the supply chain.

This is a novel approach and does not contradict other static frameworks for resilience (Christopher et al., 2003), and builds from the original “disruption curve” by Sheffi & Rice (Sheffi et al., 2005), expanding the theory by proposing mechanisms through which this behavior over time is achieved in a supply chain after a cyber-attack (cyber-resilience).

The proposal of a control structure for supply chains is consistent with other equivalent structures that have been studied in different fields of knowledge.

The explicit representation of information flows through an information flow map, has been shown to enhance team productivity and effectiveness. From this simplified system representation, four relevant insights can be derived. First, some information flows may not be present. This should trigger analyses on the need to include or exclude them. Second, some information flows will not be part of a loop. This might be the reflection of a fixed procedure in place. If there is control required on these flows, then a loop has to be completed. Third, there may be redundant information flows. This should be looked at carefully to identify the situations where this dual information flow might lead to a risky situation. Fourth, some of these information flows may not be electronic, thus not subject to cyber hacking, yet also not subject to electronic recording or with the possibility of automated control.

Some recommendations can be derived from this work.

- Understand the information flows in your supply chain.
- Control structures involving information flows in supply chains span over different areas of the company, requiring the interaction of different departments during a cyber-attack.
- The focus of the management of cyber-risks should also include the management of the systemic structure (requirements and constraints) as well as interactions, both high leverage options, and not merely the static structure and correcting of behavior.
- The process of hazard and requirements identification is an ongoing, cumulative process that is adjusted by new hazards as these are identified and integrated into the analysis.

Some of the insufficiencies mentioned in Table 2 are initially addressed through the use of this methodology for the case of supply chains. The focus is on reaction-to risk, it describes explicitly the interactions between components and can integrate redundancy as source of cyber-risks.

Conclusions and future work

This paper develops a first approach to represent the response of supply chains to disruptions caused by cyber-attacks, and proposes a structured methodology for the identification of vulnerabilities and the constraints that condition this supply chain response.

The analysis results in some general recommendations for constraints and requirements. The main areas where future work is recommended include the application to ex-post examples, the quantification of the effects of different factors and their relationship to the resulting cyber-resilience of the supply chain, and performance testing under different scenarios for varying requirements and constraints.

This approach to understanding cyber risks as a dynamic control problem needs to be implemented ex-ante for other cases, to identify constraints. There is also a potential for a network representation of the information flows, and of researching potential applications of network theory for understanding the existing relationships in supply chains.

References

Altabbakh, H., Alkazimi, M. A., Murray. S., Grantham, K., 2014. STAMP – Holistic system safety approach or just another risk model?, Journal of loss prevention in the process industries, 32, pp. 109-119.

Asbjornslett, B. E., 1999. Assess the vulnerability of your production system. Production Planning & Control, 10(3), pp. 219–229.

Carroll, J.S., 1998. Organizational learning activities in high-hazard industries: the logics underlying self-analysis. Journal of Management studies, 35(6), pp.699-717.

Christopher, M., Peck, H., 2004. Building the resilient supply chain. International journal of Logistics Management. 15(2), pp. 1-14.

Collmann, D., Krotofil, M., 2016. Cyber-physical systems security, Lecture notes in Computer Science, Vol 9100, pp.195-204, Springer, DOI: 10.1007/978-3-662-49301-4_14.

Craighead, C. W., Blackhurst, J., Rungtusanathan, M. J., Handfield, R. B., 2007. The severity of supply chain disruptions: design characteristics and mitigation capabilities. Decision Sciences 38(1), pp. 131-156.

Dederick, J., Xin Xu, S., Xiaoguo, K. Z., 2008. How does information technology shape supply-chain structure? Evidence on the number of suppliers. Journal of Management Information Systems, 25(2), 41-72.

De Oliveira, E., Werther Jr., W.B., 2013. Resilience: continuous renewal of competitive advantages. Business Horizons 56(3), pp. 333-342.

Doyle, J., Francis, B., Tannenbaum, A., 1992. Feedback Control Theory, New York, Dover Publications

Ellis, S. C., Henry R. M., Shockley, J., 2010. Buyer perceptions of supply chain disruption risk: a behavioral view and empirical assessment. Journal of Operations Management, 28(1), pp. 34-46.

Forrester, J., 1961. Industrial Dynamics, System Dynamics Series, Pegasus Communications.
Garbolino, E., Chery, J. P., Guarnieri, F., 2016. A simplified approach to risk assessment based on system dynamics: an industrial case study, Risk Analysis (2016).
Ghadge, A., Dani, S., 2013. A systems approach for modelling supply chain risks, Supply Chain Management: An international Journal, 18(5), pp. 523-538.
Ishimatsu, T., Leveson, N.G., Thomas, J., Katahira, M., Miyamoto, Y. and Nakao, H., 2010. Modeling and hazard analysis using STPA.
Johnson, N., Elliott, D. and Drake, P., 2013. Exploring the role of social capital in facilitating supply chain resilience. Supply Chain Management: An International Journal, 18(3), pp.324-336.
Jüttner, U. and Maklan, S., 2011. Supply chain resilience in the global financial crisis: an empirical study. Supply Chain Management: An International Journal, 16(4), pp.246-259.
Kang, K. M., Jae, M, 2005. A quantitative assessment of LCOs for operations using system dynamics, Reliability Engineering and System Safety, 87, pp.211-222.
Kim, Y., Chen, Y.S., Linderman, K., 2015. Supply network disruption and resilience: a network structural perspective. Journal of operations management, 33(2015), pp. 43-59.
Leveson, N., 2011. Engineering a safer world: Systems thinking applied to safety. Mit Press.
Longo, F. and Oren, T., 2008, September. Supply chain vulnerability and resilience: a state of the art overview. In Proceedings of European Modeling & Simulation Symposium (pp. 17-19).
Manuj, I., Mentzer, J. 2008. Global supply chain management strategies, International Journal of Physical Distribution and Logistics Management, 38(3), pp. 192-223.
Nair, A., Vidal, J. M., 2011. Supply network topology and robustness against disruptions – an investigation using multi-agent model. International Journal of Production Research, 49(5), pp. 1391-1404.
Petit, T. J., Fiskel, J., Croxton, K. L., 2010. Ensuring supply chain resilience: development of a conceptual framework. Journal of business logistics. 31(1), pp. 1-21.
Ponomarov, S.Y. and Holcomb, M.C., 2009. Understanding the concept of supply chain resilience. The International Journal of Logistics Management, 20(1), pp.124-143.
Salmon, P.M., Cornelissen, M. and Trotter, M.J., 2012. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP, Safety science, 50(4), pp.1158-1170.
Scholten, K., Sharkey Scott, P. and Fynes, B., 2014. Mitigation processes–antecedents for building supply chain resilience. Supply Chain Management: An International Journal, 19(2), pp.211-228.
Sheffi, Y., Rice, J., 2005. A supply chain view of the resilient enterprise. MIT Sloan Management Review. 47(1), pp. 41-48.
Sheffi, Y., 2015. The power of resilience. The MIT Press, Cambridge, Massachusetts.
Sterman, J., 2000. Business Dynamics: Systems thinking and modeling for a complex world, Boston, Irwin/McGraw-Hill
Sterman, J.D., 2002. All models are wrong: reflections on becoming a systems scientist. System Dynamics Review, 18(4), pp.501-531.
Swaminathan, J.M., Smith, S.F. and Sadeh, N.M., 1998. Modeling supply chain dynamics: A multiagent approach*. Decision sciences, 29(3), pp.607-632.
Tang, C.S., 2006. Robust strategies for mitigating supply chain disruptions. International Journal of Logistics: Research and Applications, 9(1), pp.33-45.
WEF, 2013. Building resilience in supply chains. Industry agenda report. Accessed in 12 November 2015 at http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf.
Wu, T., Blackhurst, J., O'Grady, P., 2007. Methodology for supply chain disruption analysis. International Journal of Production Research, 45(7), pp. 1665-1682.
Zhao, K., Kumar, A., Harrison, T.P. and Yen, J., 2011. Analyzing the resilience of complex supply network topologies against random and targeted disruptions. Systems Journal, IEEE, 5(1), pp.28-39.