Fachbereich Wirtschaftswissenschaft

A Decision Support System for Intermodal Logistics under Considerations for Costs and Security

Dissertation

zur Erlangung der Doktorwürde durch den Promotionsausschuss Dr. rer. pol. der

Universität Bremen

Vorgelegt von:

Julie E. Gould, M.A.

Edmonton, Kanada

Kolloquium am 5.2.2013

Angaben der Gutachter:

Prof. Dr. Hans-Dietrich Haasis
Lehrstuhl für Allgemeine Betriebswirtschaftlehre, Produktionswirtschaft und Industriebetriebslehre
Fachbereich 07
Postfach 33 04 40
28334 Bremen

Prof. Dr. Cathy Macharis
Faculty of Economic, Social and Political Sciences and Solvay Business School
Department MOSI-Transport and Logistics
Research group MOBI – Mobility and Automotive Technology
Cathy.Macharis@vub.ac.be
Building M (231) - Pleinlaan 2 - 1050 Brussels
Tel +32 (0)2 629 22 86-
Fax +32 (0)2 629 21 86

Dedication

This thesis project has been a long but rewarding journey, through which I have gained not only a deeper understanding of my topic and a broader understanding of logistics in general, but also of science, and the rewards of the pursuit of knowledge.

My sincerest thanks go to Herr Haasis, for his support and supervision, and to the colleagues at the Institute of Shipping Economics and Logistics, ISL, in Bremen, for their invaluable input over the years. To Cathy Macharis goes my gratitude for her willingness to take on a stranger and for providing a tremendous amount of feedback and encouragement, without which my thesis would not have reached where it did.

The International Graduate School for Dynamics in Logistics of the University of Bremen provided the forum for my research and the financial support to enable this work. My colleagues at the International Graduate School were instrumental in making my thesis journey so rewarding. To them I owe a million thanks for their openness and feedback, for the multitude of intercultural and interdisciplinary exchanges, and for sharing their own thesis journeys, but foremost their knowledge and experiences with me. In this group I have made life-long friendships, and these are what I value the most.

Finally, to my family, for their love during this time, for reminding what it is that is truly important, and to my husband, who saw me through it all, thank you.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AEO	Authorized Economic Operator
AVMR	Advance Vessel Manifest Rule
BASC	Business Alliance for Secure Commerce
CBRN	Chemical, Biological, Radiation and Nuclear
C-TPAT	Customs-Trade Partnership against Terrorism
FOAK	Freight of All Kinds
GP	Goal Programming
HAZMAT	Hazardous Materials
IMO	International Maritime Organization
ISPS	International Sea and Port Facility Security Code
MCDM	Multi-criteria Decision Making
OR/MS	Operations Research/Management Science
RM	Risk Management
SCEM	Supply Chain Event Management
SCM	Supply Chain Management
SCRM	Supply Chain Risk Management
SCS	Supply Chain Security
SOLAS	Safety of Life at Sea
TAPA	Transported Asset Protection Association
TEU	Twenty-foot Equivalent Unit: ISO standard 20’ (6.1 m) container
WCO	World Customs Organization
WMD	Weapon of Mass Destruction

Chapter 1 Introduction

1.1 Motivation

Transport logistics provide the backbone of the global economy. It is impossible to disassociate economic growth from the growth in international transport, as the latter provides the means of efficient production and distribution that are crucial for advancements in productivity. Demonstrating the importance of its role, the logistics industry has been growing faster than economic expansion, as individual countries are becoming increasingly specialized, and industries become centralized. Within the EU, inland transport has seen an average annual growth of over 2.5% between the years 1995 and 2006, outpacing the average annual growth in GDP in the same region, and reaching a volume of almost 2 600 million tonne-kilometres (DG-TREN 2008). Safeguarding the continuous flow of materials within and across borders is therefore critical to the global economy.

The logistics industry is seeing many changes besides rapid growth. Globalization has changed how business is done, and in the logistics industry, these changes include evolving production processes, operations, and transport processes. In relative terms, transport prices have sunk. Lower relative transportation costs have allowed production and manufacturing to be geographically spread, even over continents, creating longer supply chains. Globalization has led to a higher degree of competition, not only on price of end-products, but also on the ability to meet demands for service, quality and customization. Consumer demands change rapidly, as well, as product life cycles shorten; the ability to innovate and the flexibility to adjust quickly to these changing demands is required to stay competitive. Accordingly, supply chains have evolved to incorporate more efficient and flexible design engineering, production systems and inventory systems, and require that a greater degree of collaboration and information sharing take place between organizations along the supply chain than was seen previously.

The dynamics of the global environment in which they are embedded introduce a great number of risks into supply chains. The geographical dispersion of sourcing and

production processes makes them vulnerable to fluctuations in currency, customs procedures, and fluctuations in local and regional economic growth. Global supply chains have recently been challenged by security initiatives and procedures, especially at sea and air ports, which threaten to add to congestion at these hubs in the international flow of goods and materials. The impacts that security issues, regulations, and requirements have and will continue to have on supply chains have demanded the attention of researchers as well as practitioners. Improving the efficiency of the flow of goods and materials, and therefore the stability and competitiveness of their supply chains, remains the focus of research and practice of supply chain management, specifically where adherence to politically-driven security requirements seems to threaten the economic efficiency of logistics flows and supply chain processes, and the design of these processes does not inherently take security issues into consideration but are starting to reflect these issues to a greater degree.

One of the major issues that has arisen from the introduction and implementation of security initiatives, then, has been the perceived conflict between the cost of adherence to and certification along regulatory guidelines on the one hand, and requirements for maintaining efficiency on the other hand. The literature on supply chain management was at first applied to solve the problem of finding means of using security measures to increase the efficiency of business processes along the supply chain. The earliest solutions coming out of industry and in the literature involved either cost-benefit analysis of technical security measures, such as implementing track-and-trace technologies, as well as organizational measures, for example, tighter relationships with suppliers or customers. As researchers in supply chain management were grasping for a means to analyse security measures, frameworks of supply chain risk management (SCRM), crisis management for supply chains, or quality management were used to put the measures into a managerial perspective.

Over time supply chain security became established as both a research area and business reality of the day-to-day operations of companies and of supply chains. For one thing, the customs bodies of all important trading countries have encouraged and initiated security measures to facilitate trade. To date, 166 of 177 WCO member countries'

customs authorities are committed to the WCO SAFE Framework of Standards (World Customs Organization 2012), while the EU AEO standard effects its 27 member nations' customs proceedings. The USA's C-TPAT has thousands of member companies (USCBP 2009), and the US CSI has 26 committed customs authorities and CSI pre-screening operations cover over 80 percent of US imports before they leave foreign ports (USCBP 2008). For global supply chains, security regulations are inescapable. Studies looking at the outcomes of implementing security measures are appearing and show positive cost-benefits and highlight areas where efficiencies and improvements have been achieved by supply chains that have implemented security measures, despite the costs of these measures. The reports also give a positive impression of future developments for government-business cooperation as well as cooperation among organizations in supply chains.

So far in the literature, however, there are few governing principles that link supply chain security as a component of supply chain strategy to operational decision making. Further, a framework for analysis relating specific security measures to security performance for specific typologies of supply chains is still lacking. Due to this gap in the literature, there are few guidelines for investments into security. Instead, security measures are inherently considered as a strategic decision to commit to regulatory compliance or as an investment into quality, or security measures are used operationally as a means toward uninterrupted logistics flows. For the purpose of decision making, however, security is only beginning to be established as an organizational objective, whereby operational planning can be used to meet high-level objectives.

This work aims to create a decision support model for operational transportation planning under consideration for costs and security. First, a comprehensive literature review is offered which shows the development of supply chain security (SCS) as an area of study within supply chain management (SCM), discusses challenges and issues SCS deals with, and gives an overview of the findings to date. A framework for evaluating the usefulness of different SCM approaches is given. This framework also attempts to provide a means of operationalizing the concept of supply chain security.

Supply chain management literature has been maturing in its ability to present a framework for analysing the design of the supply chain processes in a given supply chain against its general competitive strategy. A growing area in logistics research is how logistics processes fit with supply chain strategy in value creation (Rice 2007). Following a review of the literature on supply chain security, this thesis considers how security, as a strategic component of supply chain design, might be used as a factor in the evaluation of logistics transportation alternatives. To this end, operational decision making in the context of mode choice planning is used to exemplify the role that security can take as a guiding principle. The thesis, then, contributes to this area by presenting a decision model for logistics planning within a goal-achievement context. The mode choice model developed in this thesis uses defined objectives in weighing benefits of the modal alternatives in transport planning. In evaluating the outcome of the model the strategic importance of security factors are indirectly taken into account. The changes in the alternative selection performed by the model show the magnitude of the role security factors play.

While supply chain security is the focus of the thesis, the topic is embedded in the larger picture of macro developments in supply chain management and transport systems. Logistics processes, supported increasingly by information technology and managerial expertise, are co-evolving to meet demands for speed, flexibility and responsiveness under conditions of high competition regarding costs and quality. Supporting management in dealing with these dynamics and their impact requires a great deal of decision support, an area which is co-evolving to meet the growing requirements for managerial (decision making) effectiveness.

The framework presented in this thesis is only a beginning, however. Going forward, work needs to be done towards real-time decision making in supply chains to support their ability to react faster to the information available through real-time technology. Support for high-velocity decision making situations with multiple decision makers is an area that is still evolving in the literature.

1.2 Definitions

Logistics and transport problems have historically been concerned with the "movement of materials and goods over time and space" (Sheffi 1985) to match supply with demand in place, time, quality, quantity, and price. Under consideration were mainly shipping costs and inventory carrying costs. Within this framework, the major issues looked at include the cost structure of transport and inventory, and the complexities caused by dynamic demand. The nature of the cost structure is one of decreasing marginal costs, whereby unit costs decline with an increase in the quantities of goods moved. This leads to consolidation of transport and logistics functions. At the same time, adapted inventory methods are used to meet varying demand. In order to make the logistics functions more efficient, slack in the form of inventory, and therefore, time buffers, are slowly removed, exposing processes to time risk, which can be mitigated by closer collaboration between organizations.

Logistics management continued to evolve to include more collaborative operations and integrated forms of logistics functions. One of the problems to overcome in the integrated logistics framework was moving the focus from a single organizational element in a chain to optimizing the whole system, as exemplified by the approaches of industrial dynamics and total cost approach (Croom, Romano et al. 2000). The evolution to the perspective of the supply chain focussed on the efficiency and effectiveness of the supply chain as a whole. The necessity of aligning strategy and operational planning and control functions across a supply chain required a further look at the relationships between organizations.

Supply chain management provides a framework to analyse the relationships across organizational boundaries that govern the flow of materials and information between them. As the materials flow through the supply chain, the ownership and custody of these assets passes between the organizations, as well as any risks associated with them. This change of hands has some implications for the security of the supply chain. Specifically, security is the responsibility of all parties along the supply chain, but not all parties benefit

equally when the supply chain is more secure. Therefore, supply chain security needs to be an integral part of the design of the supply chain and its strategic direction.

Security in supply chains is considered to be the set of activities, assets, and exchanged information aimed at preventing, detecting and recovering from disturbances and intrusions in the physical flow of materials and the accompanying information. A major implication of this perspective on supply chain security is a requirement to incorporate security in the design of supply chain operations that in a way that enhances their operational efficiency and sustainability. The second implication is that a continual flow of ownership must be guaranteed in order to ensure that the risks are assumed and to guarantee an incentive to mitigate any risks.

1.3 Research Questions

In the face of growing attention given to supply chain security and the mounting pressure organizations face to demonstrate the security of their logistics operations and the authenticity of the goods they need to transport, how can operational decision making support organizations in meeting their supply chain security objectives?

In pursuing this question, several subordinating questions do surface. The first question is: What are the requirements for security in the face of security pressures and regulations? As the security regulation requirements cannot be an end in themselves, it is therefore important to consider, secondly, the objectives that organizations pursue in enhancing their supply chain security, namely, what is driving organizations to invest in security? Thirdly, how can organizations get the greatest benefit from their investments into security?

In specifying the requirements and objectives of supply chain security, a framework is drawn around the problem of supply chain security in operational decision making, specifically in intermodal transport planning. In modelling the decision problem, a fourth question is raised: How can these security issues be operationalized in the context of transport decision making?

Finally, under consideration are the future areas of research that will contribute to further improvement of transport decision making.

1.4 Structure of the Thesis

In answering these questions, this thesis explores the impacts of security requirements on supply chains and logistics processes, strategically as well as operationally, and at both the managerial level as well as on the physical level. Firstly, security regulations and frameworks are discussed, including the impacts these have on the decision making function in logistics planning at the operational level. These initiatives are then looked at from the point of view of the supply chain. A background of the topic of supply chain security is given and is followed by a literature review of the state-of-the-art in supply chain security. A theoretical analysis of supply chain security is offered, and the impacts of security are analysed within this framework. The challenges related to supply chain security involve understanding: how security regulations impact the supply chain; how supply chains can derive benefits from implementing security measures; how supply chains can deal effectively with risks posed by terrorism, theft and loss; how supply chains can be made more resilient and robust in the face of dynamic risks.

After discussing the managerial challenges posed by the security initiatives, supply chain management theory is looked to for meeting the challenges posed by security requirements. Strategic objectives for implementing security measures are enumerated. Theoretical frameworks are applied to these objectives, and categories of security measures are outlined. Logistics planning in particular is considered as an operational alternative for securing the supply chain, and further, security issues are looked at in the context of a mode choice decision.

The mode choice decision in transport takes into account many different factors including relationships between partners; cost factors; quality and characteristics of the goods as well as of the transport infrastructure; supply chain configuration. This dissertation makes several hypotheses regarding impacts of security on operational decision making in logistics transport chains regarding mode choice, positing that combined transport, where feasible, is more attractive as a secure means of transport than road-only transport. A goal programming model is then proposed as a support tool for operational planning in intermodal logistics where security factors need to be accounted

for. This model is constructed to assign a series of transport consignments to different transport modes as they move through a physical transportation network. Constraints on arrival times, costs and security factors of the goods being shipped and the modes under consideration are taken into account in the mode assignment. Pre-9/11 and post-9/11 scenarios are constructed and compared for analysis. The results of the model show that security impacts can have positive as well as negative impacts on the transport process regarding costs, improvements to the security of the goods, and reliability of the shipping times. This seems to be in accord with the results coming from other studies on the impacts of security measures (Crutch 2006). Going forward it is imperative to find means for analysing investments into supply chain and logistics security to ensure that security measures are taken that match the security strategy of the supply chain regarding improving security of the goods and processes, improving business processes and making supply chain more resilient.

Figure 1.1 gives an overview of the structure of the thesis:

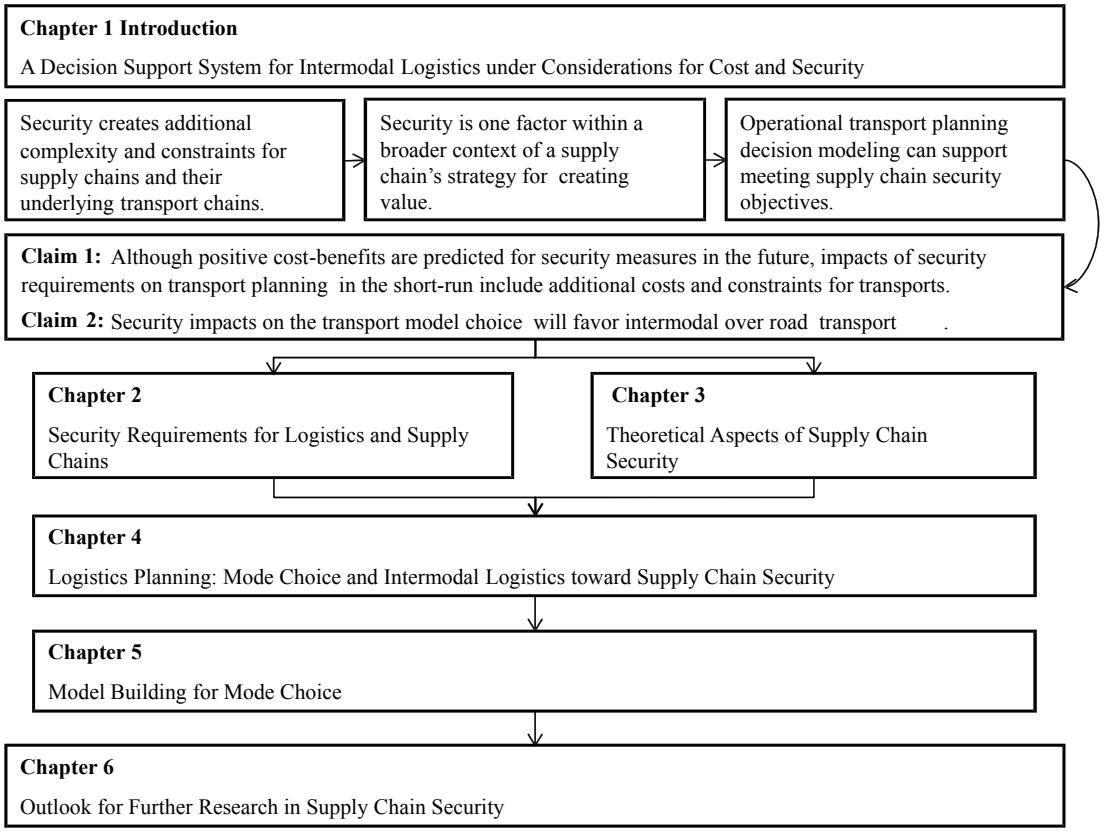

Figure 1.1 Structure of the Thesis

Chapter 2 gives an introduction and background to the topic of supply chain security. The most relevant security initiatives are detailed, followed by impacts for supply chains in terms of required investments, costs, and desirable benefits. Finally, an overview of the drivers for implementing security in the supply chain is given.

Chapter 3 gives an overview of the development of supply chain security within supply chain management theory. It provides a review of the literature on supply chain security from the perspective of several theoretical frameworks within SCM, including supply chain risk management, quality management and crisis management. The contributions and limitations of analysis of the theoretical framework are then discussed within the context of the factors driving the adoption of supply chain security. Three main objectives for implementing supply chain security are discussed. The chapter then enumerates five major categories of security measures, relating operational planning to security strategy.

Chapter 4 looks more closely at logistics planning as a security measure, and specifically at the mode choice problem. A background to the literature and the major issues and methods relating to mode choice in transport and logistics planning is given. Finally, the impact of security measures on the mode choice decision is discussed.

Chapter 5 gives an overview at a conceptual level of decision making relating to intermodal transport planning. Approaches to support the decision making function in intermodal transport are discussed, and a goal programming approach is outlined. A goal programming model is then put forward as a tool for analysis of the modal choice problem. The mode choice problem described in Chapter 4 is analysed using the model. The results are then discussed.

Chapter 6 summarizes the dissertation, discusses the major findings from the work and concludes the dissertation with an outlook for further research.

Chapter 2 Security Requirements for Logistics and Supply Chains

The political interest in the logistics and transport sector increased dramatically after the attacks on the World Trade Center in 2001. The risk of a container being used to transport illegal persons or dangerous weapons as part of a terrorist attack is a particular concern (Kumar, Jensen et al. 2008). Another threat involves the possibility of rerouting shipments of dangerous goods or hazardous materials (HAZMAT) in a malicious manoeuvre to attack a city, important facility or symbol, or another part of the critical infrastructure of a region. In response to the concern around such threats, governments have initiated security regimes to protect their borders, populations and critical infrastructure from terrorist acts involving the transport sector.

While the misuse of shipping containers and transported goods in a malicious attack is a relatively newer concern, security for the logistics sector is not a new concept. Piracy, theft, and disturbances in supply chains have long plagued the logistics industry. The political concerns, however, are being imposed on supply chains, which now face pressure to implement new security measures while maintaining cost-efficiency and strategic effectiveness.

There are several major issues that arise in the topic of security in the logistics and transport sector: the risk and the perception of the risk of terrorism, drivers for implementing security, and the value that can be generated from security measures. The risk of terrorism involving the logistics sector and the impact of regulatory and voluntary security measures designed to combat this risk need to be understood and dealt with by the private sector (Kumar and Verruso 2008). Understanding what is driving firms to implement security programmes and predicting the outcome of security programmes for supply chains in terms of costs and benefits is another key area. Finally, how value can be created from security programmes in a supply chain needs to be understood. This chapter discusses, then, the major security initiatives, the impacts these have on the logistics industry and the costs and potential benefits offered by security measures for supply chains.

2.1 The Growing Perception of Logistics Security Risks

Political interest in security in the transport sector was heightened dramatically by the attacks on the World Trade Center in September of 2001 (Banomyong 2005, Mikuriya 2007, Thomas 2008). In the aftermath of the events of 9/11, border crossings, sea ports and airports were shut down. Short-term losses in economic output due to the attack and the response to it were estimated to be close to $ 47 billion for the USA (Saxton 2002), besides the losses in property and the immeasurable loss of life. The sinking of the French tanker *The Limburg* in 2002, the 2004 attacks on the Madrid metro as well as those in London, besides the continuing piracy in South East Asia and the Gulf of Aden demonstrate over and again the vulnerability of the transport industry to terrorist attacks.

The current political perspective on security is concerned with the risk that transport systems, especially the movement of shipping containers, may be misused by malevolent groups to inflict damage on national symbols, masses of people, or on the environment (Williams, Lueg et al. 2009). The economic losses due to property damage and economic disruption of a WMD hidden in a container and detonated at a port were estimated at around $ 1 trillion by the Brookings Institution (USCBP 2006). The responsibility of deterring such terrorist attacks and establishing security standards falls to government bodies, as security measures for that purpose would not be taken up by industry where economic benefits do not directly arise from security measures. Accordingly, the aim of transport security policy is to protect against loss of life, disruption in economic trade, and destruction of critical infrastructure by providing a framework of regulation to address weaknesses and vulnerabilities that would otherwise not be addressed by firms and agents in the transport industry.

As is often the case with governmental regulations, the proposed security measures impose some barriers to trade, and thereby threaten to dampen economic activity. The goals of government-imposed security regulations seem to be at odds with the efficiency goals of supply chains (Thomas 2008). Balancing the interests of both political and economic parties is important to the future growth of the transport industry and the global economy. Moreover, matching security regulations to industry interests in improving

security will influence the level of adherence, and therefore the impact, of security measures in the logistics industry.

Security is not a new subject to the logistics industry (Hintsa 2010). Already in 19th century Germany shipments of dangerous goods were regulated to avoid possible threats to those sharing transportation routes with the carriers (Adams 1992). Besides the movement of dangerous goods, safety concerns arise in the area of road transport especially due to the sheer volume of goods that are shipped by road. Losses through damage to goods were also part of the security concept. Consequently, the more traditional safety concept in logistics translated into goods arriving at their destination in at least as good of condition as when they departed (Füngerlings 2001). Packaging and handling techniques reduce transport-related damages, especially for the problem areas of loading, unloading and transhipment of the goods. Theft and loss of goods are areas that still demand attention of shippers and their logistics service providers. Occurrences of loss and damages introduce direct costs of lost goods as well as indirect costs for lost sales, delayed production, lower service levels, and in some cases, brand recognition. It is estimated that theft reduction in the EU alone would have an annual benefit for the industry of 10 € billion per year (DNV Consulting 2005). Other estimates put the losses due to theft in transport closer to 40 € billion per year, and posit that theft is on the rise (Weise 2005). Transport security is therefore concerned with securing the goods themselves against loss through theft and damages. The risk of sabotage and terrorism can now be added as further logistic security concerns.

The sources of security risks are both internal and external to the individual organizations in the supply chain. Risk is inherent to supply chains and to supply chain processes, and can only be mitigated, but never eliminated (Svensson 2004, Peck 2005). With the more recent attention on freight transport security, additional risks are perceived involving the interception of shipments, and in using a shipping container as a Trojan Horse, a means of transporting a weapon of mass destruction, such as a CBRN (chemical, biological, radiological, nuclear) threat. Containerized transport is perceived as a particular source of terrorism risk due to the immense volume of container traffic and the complexity of container shipments (OECD 2005). 90% of the world's trade is

accomplished through the shipping container. The complexity of container movements due to the number of actors involved and resulting lack of transparency makes control via a public body practically impossible (Barnes and Oloruntoba 2005), and managing this complexity is a great task for supply chains as well. Furthermore, the focus of regulatory security measures is the safety of the surrounding environment, national symbols, human lives, and elements of the critical infrastructure. The complexity of a risk analysis of a terrorist attack is much greater than for loss of goods as the sources of this risk are external, and the potential for loss is greater. The event of a terrorist attack would result in supply shortage, lost inventory, lost sales, and the inability to receive goods from suppliers, if ports were again shut down. The firms involved in a supply chain that was misused for an act of terrorism (e.g., as a Trojan horse) would suffer from damage to their brand equity and reputation for reliability.

Due to the potential for loss and damage, the current perspective on security assigns responsibility to each partner in the supply chain for its security. Along any supply chain there can exist great disparity in the ability of the actors to make investments in security, although all of the partners in a supply chain are required to have security measures in place. Likewise, not all of the firms involved in a supply chain are as likely to benefit from compliance to security regulations, such as C-TPAT, even if their collaboration is required for preferential treatment at borders and ports, and could impact the resulting efficiency of the supply chain as a whole. In reference to the pressure to comply with security regulations, the CEO of a supply chain consulting firm was cited terming the C-TPAT as "the most voluntary, 'non-voluntary' program in the history of the US government" (Williams, Lueg et al. 2009). If security against terrorism, sabotage, theft and loss is a requirement in modern supply chains and logistics processes, it is very important to find the potential for actual benefits to be gained by employing a security programme, and how these benefits can best be achieved.

2.2 Regulatory Security Initiatives

It is a major task to reconcile the political interests of security and free-moving trade. One perspective states that the required level of security in international supply chains is a

political decision, while finding the means for achieving this level of security is left to the private sector (Dulbecco and Laporte 2005). Security programmes introduced by the United States exert more governmental and regulatory control over the flow of goods across their borders and in air and sea ports. These defensive measures are aimed at providing national protection and have made national borders less permeable. Security measures for goods being imported into that nation are subject to the Container Security Initiative (CSI), the Advance Vessel Manifest Rule (24-Hour Rule), Free and Secure Trade (FAST), and the voluntary Customs-Trade Partnerships against Terrorism (C-TPAT). They are predicted to cost the American economy alone around $ 151 billion (Bernasek 2002). The EU's proposed security measures would cost European industry an estimated € 60 billion in investment costs alone (DNV Consulting 2005).

International regulations and programmes for logistics security take a risk management perspective in attempting to protect national borders from terrorist threats. Regulatory measures are focused primarily on containerized freight transport. The volume of container traffic is immense; 90% of global trade is achieved through the shipping container, and container shipments have been predicted to exceed 600 million TEU by 2010. The global capacity of circulated shipping containers is estimated at around 20 million TEUs, or 13 million containers (World Shipping Council 2002). Containerized transport is especially a target for security, as it is conceivable that shipping units could be used to transport weapons of mass destruction, be they biological, nuclear, radioactive in nature (OECD 2005). Accordingly, security measures have targeted sea ports, as these are major hubs for container traffic. The International Ship and Port Facility Security Code (ISPS) of the International Maritime Organization (IMO), and the US Customs' Container Security Initiative (CSI) are both risk management-guided programmes covering port operations; risk assessments of shipments, facilities and personnel, as well as entry controls to the facilities are key components of these initiatives.

Regulations in the transport industry have focused until now on those logistics facilities that handle the largest flows of goods: the ports. While seaports are logistic chokepoints and therefore obvious candidates for control of the greatest percentage of goods, it is well recognized that security inspections by customs officials are inefficient and not necessarily

effective at increasing security (Sheffi 2001, Lee and Whang 2003). Moreover, security measures that result in a decline of quality aspects (reliability of delivery time, flexibility, etc.) of transport processes, which are very important to business, or raise logistics costs, act as barriers to trade and threaten to dampen economic growth (Institut für Mobilitätsforschung 2007). In order to improve the efficiency of security and customs operations at borders and ports, security measures are increasingly being pushed farther up the supply chain to the origins of the shipments. From the customs perspective, the point of origin is the point at which the exporter prepares the goods for export (Mikuriya 2007). From this point and through to the goods reaching their destination information of the goods themselves has to be available in order to ease the passage of goods through the supply chain, and especially as they pass through the chokepoint of the customs procedures. Risk assessments of the consignments are also necessary for customs to facilitate their passage at border crossings and checkpoints (Mikuriya 2007). To that end, the approach of the US Customs-Trade Partnership against Terrorism (C-TPAT) requires a self-assessment from agents involved in shipments. Due to the reliance on the previous supply chain link(s) and their suppliers, the self-assessment should result in a greater degree of interdependence, information sharing, and contact between the partners of a logistics chain, as well as between customs and business. C-TPAT certification should also result in lower likelihood of invasive inspection by U.S. Customs, both in the foreign port of departure, as well as in the U.S. receiving port. Figure 2.1 below illustrates the areas of the overseas transport chain covered by these security initiatives.

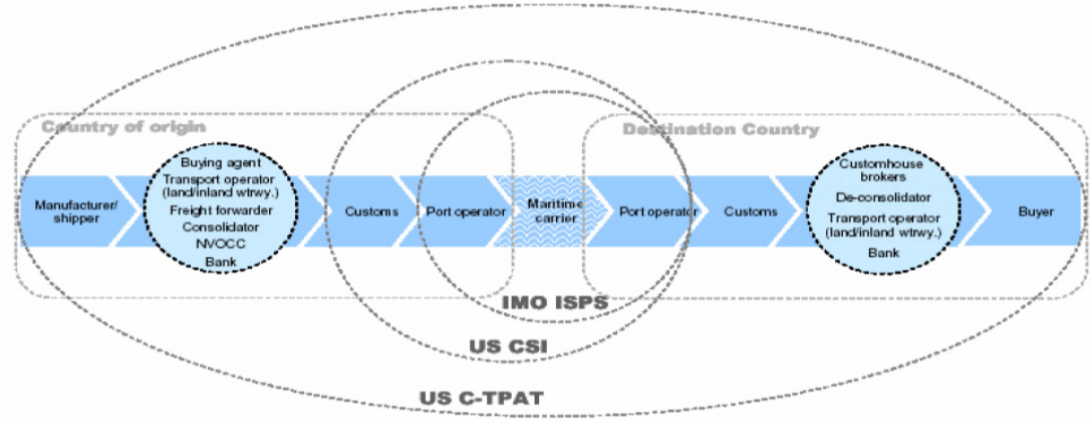

Figure 2.1 Security Initiatives along the Transport Chain (OECD 2003)

Security measures are increasingly being pushed farther up the supply chain from borders and ports to the origins of the shipments. This effort is meant to improve the efficiency of security measures and make customs clearance at points less of a chokepoint, but it requires closer collaboration between partners in the supply chain, and necessitates investments into security.

Besides customs-led security initiation, there are also industry-led security solutions. These include the adoption and application of emerging technologies such as container security devices, and organizational measures, such as the 'known-shipper', modelled after air-transport security models.

Industry-led and customs-led initiatives with the greatest impact on the actors in the logistics industry are discussed in the following section.

2.2.1 ISPS Code

The International Ship and Port Security Code was introduced by the International Maritime Organization (IMO) as an extension of the SOLAS (Safety of Life at Sea) Convention. The ISPS Code outlines security measures for ships, ports and their respective operators. ISPS came into effect July 2004. It is arguably one of the most important security initiatives as it has a great impact on the entire international shipping industry (Bichou 2004).

The ISPS Code calls for documented security plans and procedures, security assessments, automated identification of ships, ship and port employee security training and vetting, and access controls for ports. ISPS is the most implemented security measure to date, with compliance of 97% of the ports under SOLAS-compliant governments.

2.2.2 CSI

The Container Security Initiative is a U.S.-led initiative aimed at prohibiting high-risk containers from entering U.S. ports by identifying them before they are loaded onto ships bound for the U.S. To this end, data analysis of all containers departing for U.S. ports is performed to profile their potential risk. U.S. customs and border control officials stationed at foreign ports see to it that containers identified as high risk are scanned and screened at the port of departure by an official, including the use of technology for detecting the presence of radiological and nuclear activity to avoid invasive inspections as much as possible. As of 2008, 58 foreign ports representing 85% of the container exports to the U.S.A. are part of the CSI scheme.

2.2.3 Advance Vessel Manifest Rule

The Advance Vessel Manifest Rule (AVMR) or the "24-Hour Rule", has been the regulation that has effected to the greatest extent all of the shipments coming into the United States. The rule stipulates that all cargo destined for the U.S. or on-board a vessel making a call at a U.S. port must be declared to the U.S. Customs and Border Control at least 24 hours before being loaded onto a shipping vessel. This information is used for the risk profiling system as a supporting process of the CSI security programme. The 24-Hour Rule requires detailed information on the shipper, either the shipper's full name and address or an assigned identification number; container number and seal number, if the container is sealed; and identification of the receiver.

The 24-Hour Rule is meant to give U.S. Customs officials sufficient time to analyze incoming and visiting cargo shipments before their arrival in port in order to screen for terrorist risk or attempts at smuggling. However, the AVMR has the potential to negatively affect the logistics operations at ports, especially ones employing short time

windows for consignment drop-offs, such as the port of Hong Kong. Despite this significant downside, the 24-Hour Rule does lead to availability of more accurate shipping documentation earlier for actors on the receiving side of the port than was previously the case. Customs no longer accepts vague shipping notations, such as “Freight of all kinds” (FOAK). More accurate information on goods-in-transit assists to improve inventory planning along the supply chain.

2.2.4 C-TPAT

The Customs-Trade Partnership against Terrorism is also an American initiative that aims to bring industry on board with U.S. Customs and Border Patrol (CABP) through voluntary certification of supply chain actors. The prospective benefits of certification for participating U.S. companies are fewer delays by customs procedures and fewer inspections at ports. In order for importers to take advantage of the programme, however, an effort to improve and safeguard the security of the premises from which the transported goods originate has to be demonstrated. This introduces costs for additional security personnel, training and doing criminal background checks on personnel, as well as costs for physical security of facilities where containers are stuffed. Furthermore, sealing the containers with security seals is also important for participating in the programme. Importers along with their partners overseas are required to implement the prescribed security measures, even if they as exporters cannot be certified as secure operators. The “Green Lanes” at ports are to stand open to C-TPAT–compliant operators, including freight forwarders, and act like express lanes for freight, that would get through the port faster than goods not coming from C-TPAT compliant firms.

As an extension of the framework of C-TPAT, the House Regulation I, also referred to as H.R.1 or “100% Scanning Law”, was signed in July 2007, and is set to come into force in 2012. It would mean that all containers entering the US would be subject to scanning via technological means. As of 2006, only about 0.5% of the nearly 350 million handled containers worldwide were scanned, and the costs for container scanning performed in the U.S. alone amounted to about $ 380 million (Carluer 2008). By 2012, the number of

containers coming into U.S. ports is predicted to increase from about 17 million per year as of 2008 to 30 million in 2012.

2.2.5 ISO/PAS 28000

The International Standards Organization (ISO) has put out a standard "Specification for security management systems in the supply chain". The standard adheres very closely to the security principles integrated into C-TPAT and ISPS of having a security management policy in place, self-assessment, compliance with security regulations, and certification of security management. The specification calls for on-going assessment of security risks and vulnerabilities as well as monitoring of these risks. Emergency preparedness and recovery for business continuity are further aspects covered by the standard. The ISO also sets standards for implementing security devices, including container seals.

2.2.6 TAPA Transported Asset Protection Association

The Transported Asset Protection Association is an industry syndicate created as an answer to the high rates of theft of high-technology products. These high-value products are attractive to criminal organizations as they are highly mobile, and not illegal to possess. High-tech goods have a high value to weight ratio, and theft insurance, calculated on weight, does not cover their value. Moreover, additional insurance programs would not alleviate the problem, nor control the negative effects of disruptions in supply. Over 50 of the world's high-tech firms are involved in TAPA.

TAPA delineates minimum security standards for the loading and unloading, transport and storage of high-tech products. The guidelines are parallel to those of the C-TPAT, and cover the security systems for physical security of facilities, for information, documentation of processes, theft detection and reporting, theft-deterrence systems for vehicles and containers, risk-evaluation of routing, and employee background checks. Another major tenant of the TAPA guidelines is to maintain secrecy of information on transport schedules and planned routes as well as having contingency plans for rerouting

when necessary. Tracking and tracing is also employed to validate the security of goods en route.

2.2.7 EU Directives for Transport Security

The European Community has set for itself the goal to improve the security of all cargo, and consequently all operators as well as the infrastructure which directly relates to the functioning of the supply chain, i.e. terminals, distribution centres and inland ports. The EU security proposals cover all areas of inland transport including road, rail, inland shipping, and short-sea shipping as well as maritime shipping. Security of infrastructure as well as that of logistics and transport processes is taken into account.

Creating harmony with international regulations was one of the biggest issues considered by the European parliament in connection with formulating an action plan for transport security, while at the same time supporting the specific needs of the industry within the EU. Another issue was to make security of transport processes feasible while not burdening the industry with undue costs and compromise the competitiveness of the actors. Additionally, the importance of information security factored into the discussions on creating viable security regulations. Finally, security measures were sought that could provide value by inciting improvements to supply chain processes that would promote their efficiency.

Maritime transport security was approached by the EU's COM(2003)229 and REGULATION (EC) No 725/2004, both of which were meant to be harmonious with the IMO SOLAS Convention and the ISPS Code. The Regulation governs the interface between ships and ports, and considers ships as potential bringers of danger. The Proposal for Direction 2004/0076 put forward guidelines for EU regulations of the security of sea ports. Sea ports are considered to be gateways into the EU, and therefore sensitive areas in need of regulation. Port infrastructure and equipment are considered critical to the economy of the EU, and are therefore come under the protection sought by the security regulations. Put forward in February, 2004 the proposed directive for Port and Ship security aims include:

1. Port security complements maritime and ship/port interface security and ensures that these security measures are reinforced by security measures in the entire port area;
2. A port security assessment decides what measures are required, where and when;
3. Security levels distinguish between normal, heightened or imminent threats;
4. A port security plan outlines all measures and details for enhancing port security;
5. A port security authority is responsible for the identifying and implementing appropriate port security measures by means of the above mentioned assessment and plan;
6. A port security officer coordinates development and implementation of the port security plan;
7. A port security committee provides advice to the responsible authority.

Training and control will support implementation of the required measures. The costs that are incurred by the security measures are to be carried by public regulatory bodies.

In order to achieve a higher level of security and to avoid a doubling up of efforts, it was put forward that targeting the ports only is faulty, and that a comprehensive security regime will start inland, or farther up the transport chain, in the same manner that C-TPAT aims to do. It is concluded that along an intermodal transport chain, a risk posed at any point along this chain will be a risk for the entire chain. EU security regulations, as described in Communication COM(2006),79 on enhancing supply chain security, respond to security issues in inland transport and logistics, not the least of which is the high level of theft; concentration of security efforts at ports is not responsive to this need, but needs to consider especially road and rail freight transport. In the same way that ports are considered to require security measures, inland terminals – rail yards, inland navigation terminals, consolidation centres - are also considered to be vulnerable. For intermodal transport, it has been proposed that the greatest vulnerabilities are found at the connections between the modes (OECD 2005).

The EU's answer to the security regulation problem was to create a voluntary scheme, rather than mandatory security rules, since "voluntary programs encourage collaboration with Customs and allow for flexibility of security policies and procedures that would not

be possible under a regulated program" (Fletcher 2007). Like the C-TPAT, the EU directive proposes: risk analysis and assessment, establishing a limited number of security levels, and integration with international security measures. Furthermore, the EU concept attempts to cover all operations and agents involved in the supply chain: "The standards will cover every operator in the supply chain and make each one responsible for its own security, including shippers, transport and forwarding companies, warehouses and storage facility operators" (EU 2006).

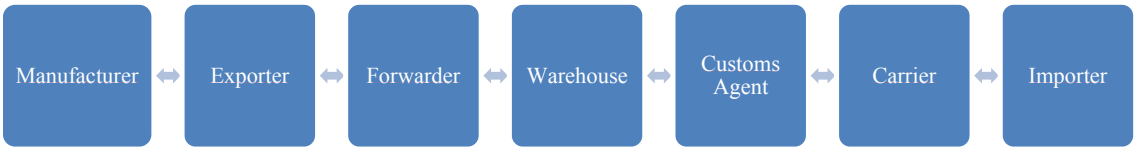

Figure 2.2 Operators Covered by the EU's AEO Customs Programme (EC 2006)

Central to the EU directive on transport security is the creation of the "secure operator" or Authorized Economic Operator (AEO) status[1], an extension of the "known shipper" or "known consignor" concepts from air-transport security. Similarly to air freight transport, the operators voluntarily taking part in the initiative are offered faster throughput at terminals within the EU as well as on its borders. When targeting shipments for security controls, EU member states are to assign AEO consignments with a lower risk score. If a consignment from an AEO is subjected to inspection, the consignment should be given priority over non-AEO consignments, and the control should be performed as quickly and conveniently as possible (EC 2006).

The development of the AEO approach for supply chains supports the increased visibility of actors in the transport industry and transport processes that is required to improve their security. AEO certification is one way for EU customs officials to recognize the operators responsible for the freight moving across EU borders. The processes of received AEO certification is simplified for operators who already have certification along standards ISO, ISPS, C-TPAT, EC Secure Operators, or a comparable concept (EC 2006). Requirements for investment on the parts of the firms to achieve AEO status, however, are

[1] Criteria for adherence are laid out in Reg. (EC) 648/2005.

still significant. Areas for investment include: technology (i.e., e-seals, ICT), personnel (i.e., additional security personnel, security awareness training, background checks), facility security (closed-circuit television, access controls). Other non-investment costs, referred to from now on as unrecoverable costs, also occur, such as compliance fees, and security fees at port and transhipment facilities. Estimates for average investment costs for small, medium and large firms are made to be € 50 000, €135 000, and €300 000, respectively (DNV Consulting 2005). Estimates of aggregated security costs for the logistics industry amount to €60 billion for a mandatory security regime. Despite potential for economies through increased efficiency resulting from improved processes and tighter collaboration between supply chain partners, these costs are not recoverable: "There is no escaping the fact that security will add a further line in the accounts of companies involved in international trade. The trick will be to ensure that the costs are minimised and do not impede trade or the overall economic viability of conducting international business" (European Shippers Council 2004).

The approach of the EU to security requirements mirrors that of the U.S. in desiring to protect citizens and critical infrastructure, while at the same time safeguarding economic operations and flows of goods and people. Besides security, the European Union is also concerned with privacy of information. While parties on both sides of the Atlantic agree that proper documentation and sharing of information are essential to security efforts, EU members' criticisms of the US security initiatives are often directed at the potential disclosure of this sensitive information, fearing that sensitive market information might be used to change the competitive landscape, where individual firms may lose some of their competitive advantage, or that it would actually offer criminals more opportunities to plan an onslaught with accurate schedules of shipments. A further concern in implementing security regulations was due to the costs involved, and the disinterest in making the European transport and logistics industry less competitive. European policy tends to be protective of their small and medium-sized enterprises, which make up a good portion of the firms in the logistics industry; over 99% of the estimated 4.8 million enterprises potentially affected by an EU security policy in the EU 25 region are SMEs (DNV

Consulting 2005). Any security schemes put into place by the European Commission has to respect the needs for security, privacy of information, and economic viability.

In sum, the EU's approach to security in the supply chain is based on the concept that, although supply chain management (at an operational level) is an industry's responsibility, a state's responsibility is to overcome the vulnerabilities that self-regulation in the industry would leave. Moreover, the state can provide incentives for companies to invest in their logistics security (such as "Green lanes" at ports) that would speed up adoption rates of security measures throughout industry. Therefore public-private partnership is necessary for both the political and economic goals of security measures to be realized (Sheffi 2001, Wolfe 2004, EC 2006).

2.2.8 WCO SAFE Framework of Standards

The World Customs Organization (WCO) has made its own contribution to the security of global supply chains with SAFE (security and facilitation in a global environment) Framework of Standards, which was adopted in June 2005 (Mikuriya 2007). The perspective of the WCO relies its long history of creating international agreements covering the transport of goods across borders; in this perspective, customs becomes a service provider in facilitating trade, and serves national and international economic and political interests by identifying illegitimate and fraudulent trade. Within the SAFE Framework of Security, the WCO has set "the principles and the standards and presents them for adoption as a minimal threshold of what must be done by WCO Members" in regards to secure global trade (World Customs Organization 2007). The principles outlined by the SAFE Framework are parallel to those of the American C-TPAT and CSI programmes, namely: advanced delivery of cargo information to customs in an electronic form; a risk-management approach to dealing with security threats; inspection of outgoing cargo using non-intrusive technologies at port of departure; and benefits involving smoothed customs procedures for consignors who comply with the SAFE Framework, in this case voluntarily.

As was discussed above to be the case with the EU directive for security, the guidelines outlined in the SAFE Framework for industry actors are achieved through the creation of

the AEO status. Of course, the SAFE Framework has in its focus the role of the customs bodies of the individual nation states and will only achieve the goals set forth by the SAFE Framework if customs procedures support the scheme and operators in industry achieve certification for AEO status. The SAFE Framework, therefore, calls for cooperation and mutual recognition between customs bodies of WCO countries, and cooperation between customs bodies and industry (Mikuriya 2007). The benefits for operators in validating their AEO status are lower risk-assessments at borders, fewer inspections, and expedited customs procedures (Fletcher 2007). These benefits, which are the main incentives for private business to partner with customs in the scheme, depend to a great extent on the cooperation between nation states regarding customs, namely that both AEO status and customs clearance are mutually recognized by WCO member nations. Therefore, the WCO concerns itself with the network of interactions and agreements between customs departments regarding advanced cargo information, risk assessment, and international cooperation to facilitate legitimate and secure trade.

2.3 Impacts of Security Measures on Supply Chains

Security initiatives have a great impact, directly and indirectly, supply chains. Positive effects of security initiatives will raise the level of security in a supply chain, for example, by lowering risk of intrusion, smuggling, or theft. Improving the effectiveness and efficiency of business processes in the supply chain is another possible positive impact. And lastly, security measures have the potential to improve the ability of a supply chain to detect a security breech more quickly and react more quickly to security events that do happen to limit their impacts (Banomyong 2005). Security initiatives, however, have the potential to result in lower reliability (Voss, Closs et al. 2009), congestion at logistics hubs and especially at ports, and overall higher logistics costs (Banomyong 2005). These negative impacts are summed up in Figure 2.3:

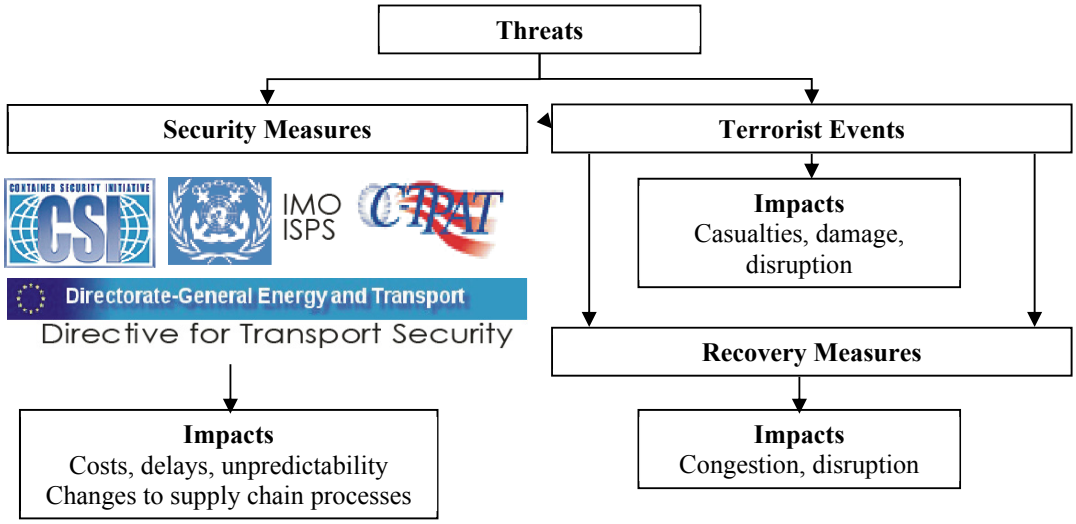

Figure 2.3 Impact of Security Measures, adapted from Wolfe (2004)

It is also important to point out which actors are affected by security risks and regulations. Looking at the transport chain as depicted in Figure 2.2, the areas impacted by security measures can be identified. This is depicted in Figure 2.4.

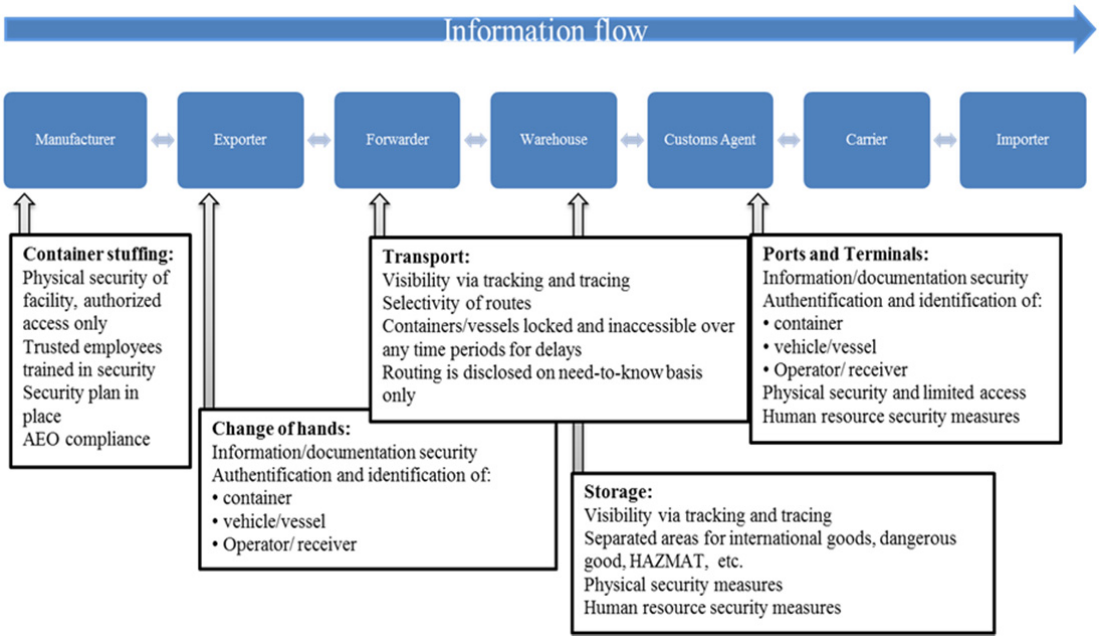

Figure 2.4 Impacts of Security Regulations and Initiatives on the Transport Chain

Clearly, the costs for security measures (apart from those financed by public bodies) are borne by shippers, LSPs, and transport operators. Initially, regulatory security initiatives resulted in higher costs and a great deal of expense as shippers, logistics operators, ports, governmental bodies, among other actors in related industries, sought certification in adhering to the security initiatives as they were first introduced. The challenge at this stage was dealing with financing these new costs (Dulbecco and Laporte 2005), and one of the foremost research questions dealt with finding a means to gain economic advantages to balance out the costs of compliance with the new security initiatives by creating efficiencies (Bichou 2004, Gould 2007). The cost of adhering to security measures can also divert efforts and resources towards compliance and certification and away from innovations that may be more beneficial (Burgess and Singh 2006). In terms of security, the issue is that investments made for adherence to security initiatives will not necessarily lead to more security in the supply chain. One critic of the C-TPAT programme, for example, found it useful in calling attention to global partnerships, but not very effective in getting firms to look at interactions between its own business units in order to deal directly with root causes of disruptions (Varkonyi 2004). The net benefits of security improvements can only be distinguished at the supply chain level, based on the overall performance of the supply chain under conditions of heightened security requirements. Since financing security measures has since been incorporated in the charging policies, the new challenges of supply chain security deal with getting competitive advantages and building capabilities out of investments into supply chain security (Fletcher 2007).

2.3.1 Costs of Security Measures for Supply Chains

One of the major objections by industry against government-introduced security measures arose from the cost to the industry. The logistics industry is largely comprised of small to medium-sized companies, and, in the case of voluntary security schemes such as the C-TPAT and WCO SAFE, extra costs for security would make compliant companies less competitive from a cost perspective against their non-compliant competitors, especially if no other benefit materializes. As the supply chain security concept covers all members of the supply chain, manufacturers will also be expected to implement security

measures that comply with international regulations and initiatives. As a way to offset the disadvantages of the costs, firms certified with C-TPAT or as an AEO are offered preferential treatment by customs and at ports and borders, such as in the FAST programme for trans-border transport between the U.S. and Canada, or the proposed "Green lanes" at marine terminals.

Security programmes such as FAST, C-TPAT and the SAFE Framework of Standards offer benefits for certified logistics operators, shippers, and service providers. It is quickly apparent, however, from looking at the literature on the possible impacts of security measures that much of the discussion is qualitative, with only growing tendency for qualitative assessment studies. Some exceptions were found in quantitative studies, especially surrounding calculations of the benefits of applying specific technology, such as RFID-enabled e-seals, as is the case of the hypothetical scenario by Lee and Whang (2003). Another study on the impact of the cost of security was done by Sheffi (2001), which looks at the loss in profit incurred due to two security measures: application of RFID technology, and multiple sourcing, including local sourcing.

The cost of implementing security measures can fall into several categories: recoverable costs, unrecoverable costs, and costs of doing business. In the first category there are costs incurred by firms that can potentially be offset by economic benefits from reductions in theft, loss, variance in lead time, stock-outs. In this case, security measures act as a kind of insurance against disruptions in general (Sheffi 2001). Other quantifiable benefits are foreseeable from increased communication and collaboration between suppliers and customers along the supply chain from visibility technology (tracking-and-tracing technology, SCEM systems) and collaborative risk assessments and contingency planning, which would decrease reaction time and improve decision making in the face of an unplanned event (such as a lost container) or another kind of disaster (see Chapter 3 Theoretical Aspects of Supply Chain Security).

Some security-related costs, however, are not recoverable. The most significant of these appear in the form of "operational redundancies" (Sheffi 2001), such as the necessity of maintaining higher levels of safety stock, local rather than global sourcing, and using a multiple sourcing strategy rather than single sourcing. Global sourcing and lean

management principles have also come under a great deal of scrutiny, especially in cases of cross-border trade where there is a great distance and hence longer lead times and potential for disruption between supplier and buyer. Other unrecoverable costs arise from traditional security measures, for example facility access controls (perimeter fencing and ID readers), CCTV, additional security personnel, etc. (Wolfe 2004). Such measures provide security benefits at specific locations, but minimal economic benefits and pose a burden on industry and trade. Costs that stem from meeting the specifications of security programmes, even where more significant investments into security measures, security systems and procedures, are required and can be considered as the "costs of doing business" in the post 9/11 environment under the threat of terrorism.

A report by DNV Consulting, looked at the potential impacts of security legislation in the EU (DNV Consulting 2005). They found that, in the case of a mandatory security scheme affecting an estimated 4.6 million companies that would comply with the EU regulations, the costs of compliance would amount to between 40 and 50 billion Euro, or 0.5% of the region's GDP for initial investment costs, where annual costs are comparable to the investment costs. The same report found that security costs are not evenly distributed among corporations; small companies employing between 10 and 50 workers bear the greatest costs as a percent of turnover of around 1% for investment costs and annual costs for security, while large corporations with more than 250 employees would be paying less than 0.5% of their turnover for security costs.

Table 2.1 Total Cost to Industry Covering All Operations (DNV Consulting, 2005a)

	Number of companies	Costs per company	Maximum costs
Micro company (<10 empl.)	4,208,300	€ 5,000	€ 21 billion
Small company (<50 empl.)	424,800	€ 50,000	€ 21 billion
Medium company (<250 empl.)	98,008	€ 135,000	€ 13 billion
Large company (>250 empl.)	19,335	€ 300	€ 5 billion
Total	4,750,443		€ 60 billion

Looking into the logistics sector specifically, we can see that some logistics operators face far greater costs than others; inland shipping faces far steeper investment costs and

annual costs of € 8000 per company than road transporters and other operators in the micro category, while warehousing companies face larger costs relative to other operators in the category of large companies. The costs per company in € 1 000 are given in the figure below.

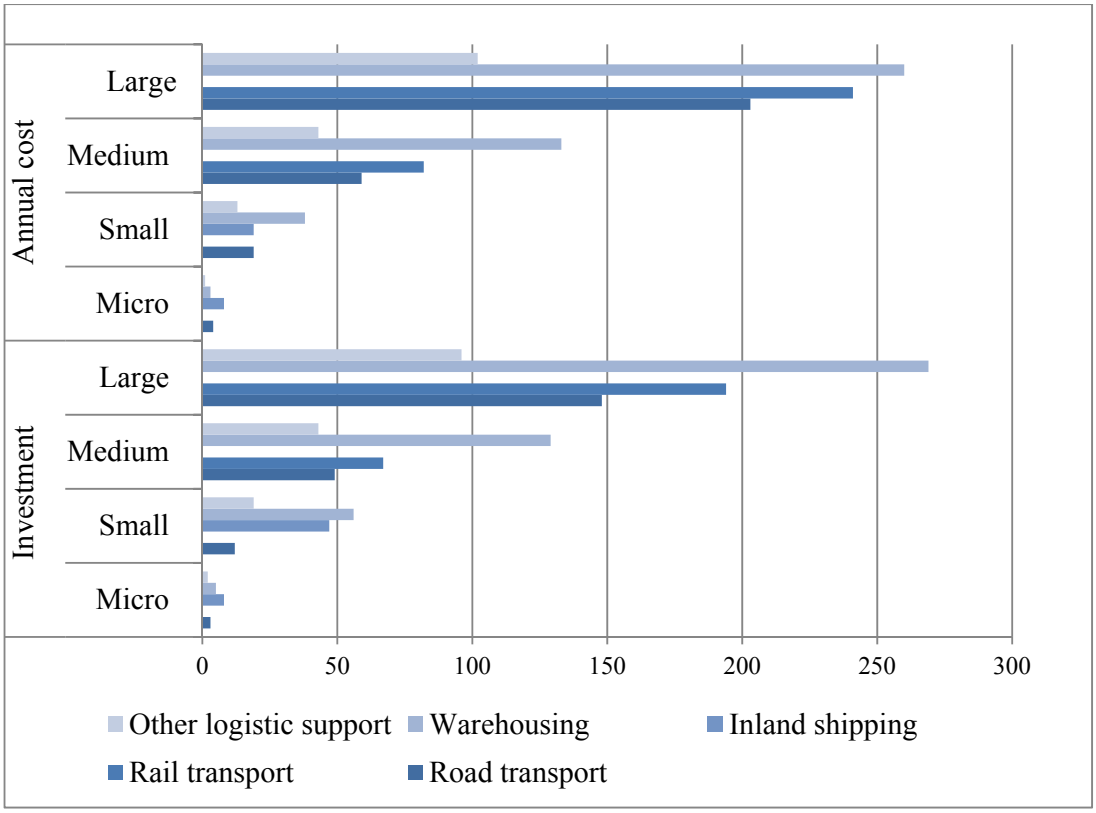

Figure 2.5 Investment Costs and Annual Costs of EU Security Measures per Company in € 1000, adapted from DNV Consulting (2005a)

Broken down by sector, the cost to industry of the mandatory scheme is also borne disproportionately, as companies in manufacturing and construction would bear over 92% of the costs, and the logistics sector just over 7%.

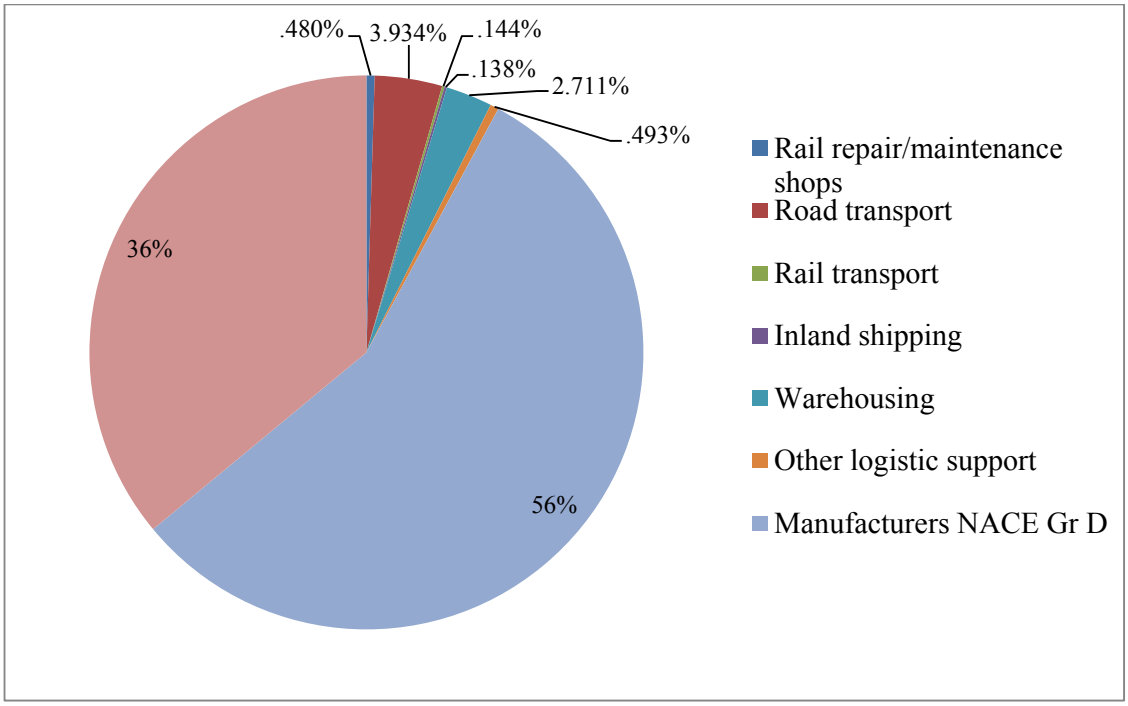

Figure 2.6 Total Costs to Industry of EU Security Regulations by Sector, adapted from DNV Consulting (2005)

The costs for mitigation measures are made up of costs for: general system requirements, such as security self-assessment and documentation of security measures and procedures; procedural security, such as response planning for security breaches, implementation of e-seals, inspections, and detection of anomalies; human resource security, such as background checks and security training; physical security and access controls, which ensure that cargo, cargo transport units, vehicles, and facilities are protected from unauthorized intrusions; and lastly, measurement and analysis of security measures. The portion of the mitigation costs for each category of mitigation procedures is demonstrated in Figure 2.7. As can be seen, the greatest percentage (between 70% and 90%) of the mitigation costs arise in physical security and procedural security measures that are specific to an organisation's activities and industry, such that costs differ between transporters, warehouse operators, freight forwarders, and shippers. Sources suggest that the cost for physical access controls amount to between 5 % and 10 % of their investment costs (Logistik Heute 2008).

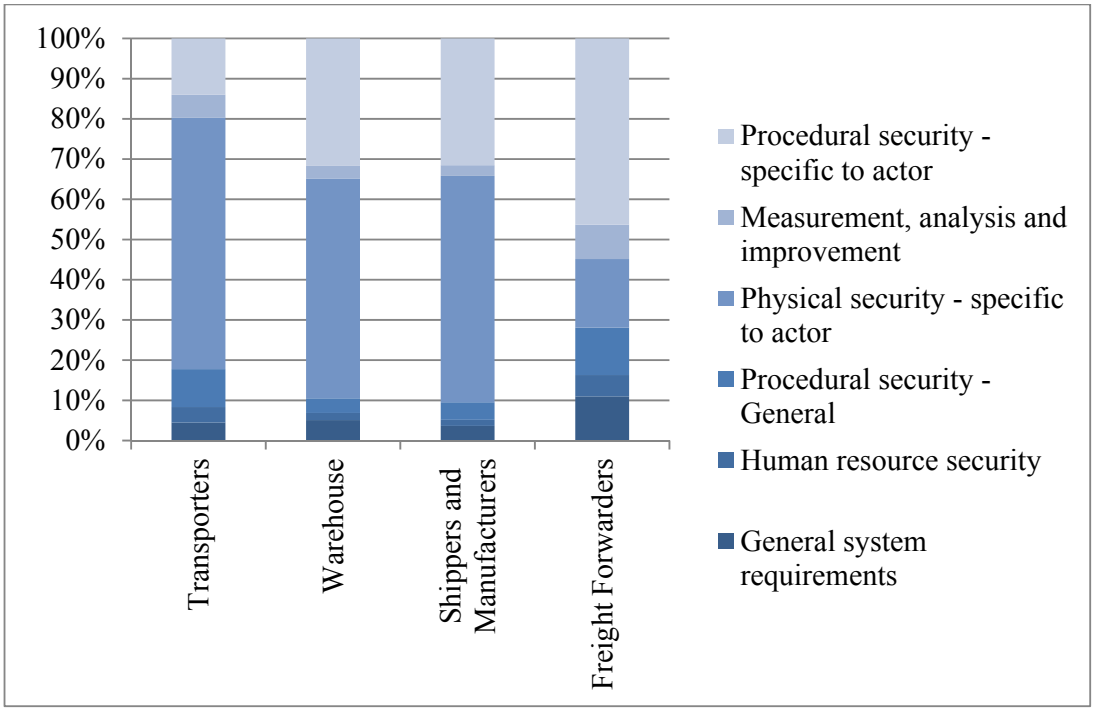

Figure 2.7 Breakdown of Security Costs by Mitigation Category[2]

It can be concluded from the picture above that the implementation costs of security measures as well as impact on the security and benefits that can be achieved are specific to the actor and the service that actor provides. Further, it can be stated that security measures cannot be generally created for all sectors of industry, but require fitting to industry-specific and service-specific processes.

DNV's study of the impacts of EU security legislation further suggests that it is expected that not all firms would participate in a voluntary security scheme, and the highest percentage of participation would occur in large firms, while the weakest levels of participation would occur in the micro firms.

[2] Costs include both implementation as well as maintenance costs, as given in the same study.

Table 2.2 Participation in Voluntary EU Security Scheme (DNV Consulting, 2005a)

	Micro			Small			Medium			Large			Total		
	# comp.	%	# particip.	# comp.	%	# particip.	# comp.	%	# particip	# comp.	%	# particip	# comp.	%	# particip.
Shippers	3693000	15	553950	345500	25	86375	93000	65	60450	19000	95	18050	4150500	17	718825
Transporters	458300	30	137490	50300	50	25150	3008	80	2407	335	95	318	511943	32	165365
Forwarders	54000	20	10800	5000	20	1000	1000	25	250	0	0	0	60000	20	12050
Terminal operators	3000	10	300	24000	30	7200	1000	80	800	0	0	0	28000	30	8300
Total	4208300	17	702540	424800	28	119725	98008	65	63907	19335	95	18368	4750443	19	904540

The same study showed that the potential total cost to industry in the EU would be much less than under a mandatory regulation. Where both the average upfront investment costs and the average annual costs per company are similar to those given in Table 2.1 above, the total cost to industry amounts to around 12 billion Euro, rather than the 60 billion Euro as shown in Table 2.3 below:

Table 2.3 Total Cost to Industry of Voluntary EU Security Scheme (DNV Consulting, 2005a)

	Number	Costs	Maximum costs
Micro company	665 485	€ 5,000	€ 3.3 billion
Small company	86 225	€ 50,000	€ 4.3 billion
Medium company	24 805	€ 135,000	€ 3.4 billion
Large company	3 601	€ 300,000	€ 1.1 billion
Total	776 440		€ 12.1 billion

The magnitude of the costs for implementing security to firms and to the logistics and manufacturing industries underscores how important it is that real, measurable benefits materialize as of result of implementing security measures. For one thing, firms need to benefit from their participation in security initiatives, and for another, there should be positive improvements in supply chain performance.

2.3.2 Potential Benefits of Security Measures for Supply Chains

Security measures should result in a measurable decrease in security risks of theft, counterfeit and sabotage, terrorism, smuggling. Specifically the risk of a terrorist attack involving transports and an improvement in a firm's ability to protect itself against significant loss to their image and brand name in the event of a realised or attempted terrorist attack involving goods produced or handled by or belonging to that company. In the worst case that an undesirable event should occur, security measures in place should offer heightened capacity for early detection, and through especially risk analysis and contingency planning, ability to react faster and with less loss than it would otherwise be able to. In their study of the impact of voluntary compliance with the Business Alliance

for Secure Commerce (BASC),[3] Gutiérrez et al. investigated benefits of implementing security measures for participating firms. They categorized security benefits in three main areas: direct improvements in security, which could be measured statistically in terms of intrusions, theft, tampering, and other anomalies; heightened efficiency of business processes, including heightened image and perception of credibility; and increased ability to react in a crises situation (Gutiérrez, Hintsa et al. 2007). The authors found the benefits rated to be the most important were reducing a firm's vulnerability to smuggling and theft, and improving business processes, including an improvement to the firm's image of credibility. Improving reaction to a crisis situation was rated as both less important and less well achieved than other types of benefits (Gutiérrez, Hintsa et al. 2007). IBM's research found key benefits to be increased efficiency of processes and enhanced supply chain resiliency. Efficiency improvements include better inventory and customer relations, and improved asset visibility (Fletcher 2007). A content analysis study by Autry and Bobbitt (2008) on supply chain security research reported identifying outcomes for performance, including customer satisfaction and supply chain continuity.

In an analysis of cost-benefits of security measures, their contribution to the value of a company's intangible assets is an important aspect. Gutiérrez et al. (2007) found that of all expected and realized benefits of implementing security measures, improving the company image and credibility is the most important. This was supported by Whipple et al.'s research that security was considered a means of protecting a firm's brand or reputation (Whipple, Voss et al. 2009). To underscore the value of credibility, publicly-announced supply chain glitches were found to have caused a decrease of over 10% in shareholder value for the companies that experienced the glitches (Hendricks and Singhal 2003). Supply chain glitches considered by the study included an inability to meet demand due to part shortages or production problems. Potential benefits for companies for implementing security measures therefore include the possibility to build up their reputation and brand image as a company that takes proactive measures to ensure the security of goods and products they produce and transport, and serve as a signal for

[3] BASC is an anti-smuggling security initiative involving Latin American importers to the USA. For more information on the BASC, see World BASC Organization. (2005). "BASC - Business Alliance for Secure Commerce." Retrieved May 01, 2010, from http://www.wbasco.org/index-eng.htm..

current and potential supply chain partners. Reputation for reliability is a key intangible for logistics service providers. Certification along the guidelines of security programmes such as the C-TPAT, as an AEO, or with ISO/PAS 28000:2005 provide immediate recognition of adherence to at least minimal standards for secure transport operations in the same way the TAPA certification has provided for high-tech goods in the past. LSPs with overseas operations and especially involving trade with the U.S. will find that security certification will provide some level of recognition of value-add. Fletcher found that participation in an AEO program to be a major criterion for companies assessing their suppliers or selecting new ones (Fletcher 2007). These "reputation benefits" arise in the case of a voluntary security regime.

Border crossings represent a major potential bottleneck for logistic flows, and thereby business processes. For this reason, the first potential benefit offered by customs bodies for operators complying with security programmes is faster processing by customs agencies. The EU AEO programme as well as the US C-TPAT programme aim at facilitating the movement of goods at air and sea ports in this way. These programmes offer lower risk scores and priority handling in physical inspections and documentary controls for certified operators, which means that the goods spend less time being processed by Customs and experience fewer inspections and customs-related delays (EC 2006, USCBP 2009). One study on the impact of C-TPAT certification by Sheu et al. (2006) found that the studied supply chains saw positive results in terms of fewer port inspections, fewer delays and lower costs, as well as tighter collaboration in partnerships between actors in the supply chain surrounding supply chain security. The value of C-TPAT compliance improving logistics security is still unclear, and the authors found that no real potential was seen in the near future for LSPs to turn their supply chain security programme into value-added service activities. However, increased supply chain visibility with better information, tighter collaboration with partners in the supply chain, and partnership with government on security show a great deal of promise for improving efficiency of cross-border supply chain processes.

The use of technology such as RFID has also shown significant potential to create efficiency gains for cross-border transports of goods while increasing security through

higher visibility. One study by A. T. Kearney Consulting found savings estimates at over $1000 per RFID-equipped container for imports into the USA (A. T. Kearney 2005). These benefits would only increase when added to the promised "Green lane" treatment RFID-enabled consignments would receive at ports, allowing their quick release by customs. Measurable decreases in lost goods and theft should also occur with heightened visibility and ownership. Combined with lower risk of delays for inspection at borders and customs controls (the "wild card" in international shipping), the supply chain would benefit from lower safety stocks, stock-outs, and the resulting improved service levels due to reliable delivery, which in turn offset the cost of carefully planned security measures. Moreover, supply chain visibility is enhanced where information on goods-in-transit is transmitted through the supply chain. Security measures have stipulated that correct documentation of the shipment must precede the goods. Receiving information on in-transit inventory provides a further means of reducing stocks, lowering the incidence of receiving orders incorrectly and allows for tighter planning overall. Implementing Track-and-Trace technology enables real-time information sharing on in-transit goods, further enhancing inventory planning.

One final long-term benefit of the security programmes is the potential to align regulatory customs procedures and trade more closely. The C-TPAT and AEO programmes offer a contact person in customs to certified operators (EC 2006). While advanced submission of shipping documents is already an important part of the C-TPAT, the EU AEO programme is also concerned with making advanced electronic submission of documents more beneficial, and is going so far as to look into allowing summary declarations instead of requiring full disclosure of shipment elements, giving advanced notice to AEOs of planned customs controls, and release of consignments by customs prior to their arrival/departure (EC 2006). Going forward, with more operators applying for security certification, there is potential for a greater partnership between regulatory customs bodies and operators in the transport and logistics industry[4] (INTEGRITY and

[4] Thibault posits public-private coordination as a benefit for SCS, as cited in Williams, Z., J. E. Lueg, R. D. Taylor and R. L. Cook (2009). "Why all the changes?: An institutional theory approach to exploring the drivers of supply chain security (SCS)." International Journal of Physical Distribution & Logistics Management **39**(7): 595 - 618..

SMART-CM 2008). Moreover, mutual recognition by customs bodies of security programmes such as the EU AEO, the WCO's SAFE, and C-TPAT initiatives will make adherence to security programmes and certification simpler and more beneficial. For example, the EU member states are to take compliance with comparable security standards into account to simplify the certification processes for applicants of the EU customs authority's AEO certification programme (EC 2006). In this way, customs will facilitate secure trade, rather than impede trade (Mikuriya 2007, INTEGRITY and SMART-CM 2008).

One of the major issues going forward will be allocating benefits of security across supply chains (Manuj and Mentzer 2008, Laeequddin, Sardana et al. 2009).

Assessing the value of security measures is, then, the first step to receiving compensation for investment. Gutiérrez et al showed that some companies were able to benefit to a much greater extent from their security investments, while other companies investing the same amount or more saw far less improvement. Some reasons include the difficulties in measuring security or business process improvements. Assessing benefits also depends greatly on the risk perception that a firm has; the greater the perceived risk a company faces, the greater the benefits resulting from security investments, and vice versa. The authors pointed out that the disparity of benefits between actors in the supply chain made assessing the cost-benefit analysis difficult (Gutiérrez, Hintsa et al. 2007). Plotting the number of security measures taken against the benefits that these firms received revealed little in the way of a direction connection between investment and benefits, as shown in the figure below:

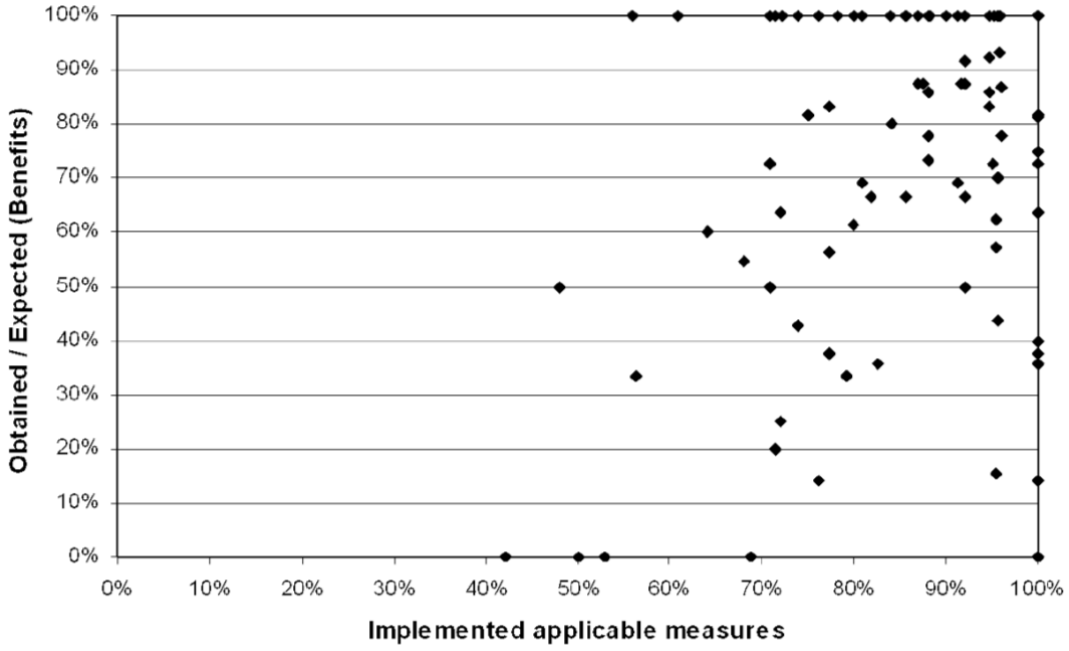

Figure 2.8 Relationship between implemented applicable security measures and obtained benefits (Gutiérrez, Hintsa et al. 2007)

The value of investments into security measures is consequently a topic for further research. Nevertheless, programs for supply chain security are still treated as strategically important and are being implemented. Since the benefits from investments into security are not as yet easily quantifiable, and the performance of security measures is difficult to measure, questions arise as to why firms do adhere to voluntary security measures and what is driving investment into security.

2.3.3 Drivers of Security Programs

One important driver of security programs is a heightened awareness of the risk of catastrophic events (Cavinato 2004, Knemeyer, Zinn et al. 2008). Government regulations are also a major reason for firms' investing into security programs, and specifically into certification and compliance (Williams, Lueg et al. 2009). This is true especially for shippers with time-sensitive production and inventory systems as well as for operators and LSPs responsible for bringing the goods across international borders, as these groups are

vulnerable to any delays due to customs procedures and inspections. Time-sensitive supply chains can therefore also benefit more from faster processing and handling by customs at ports. Another driver is the institutionalization of certification and compliance with international security regulations. Pressure from customers, suppliers or even competitors to comply with security "norms" is one reason why LSPs invest in security programs, rather than the impact of that investment (Peleg-Gillai, Bhat et al. 2006, Williams, Lueg et al. 2009). Reputation is a major driver for LSPs to invest in security, and in achieving certification in compliance with international security regulations in general (Peleg-Gillai, Bhat et al. 2006).

In sum, security is a requirement for doing business. The question is not whether or not to implement security measures, but rather what can be gained from investments into security and how these benefits can be realized. There seems to be a consensus that security performance will differ between firms who will take a leadership position in security capabilities and firms who are followers, separating secure supply chains from highly secure supply chains; those companies who are already seeing benefits from their security programs are "supply chain security leaders" (Peleg-Gillai, Bhat et al. 2006, Hameri and Hintsa 2009, Williams, Lueg et al. 2009). Furthermore, the performance of security initiatives needs to be measurable. How can security as a criterion of supply chain performance be evaluated?

2.4 Summary of the Research Problem

Security is a requirement for doing business in the world post 9/11. Terrorism continues to pose an underlying threat, and governments have taken action to see that the logistics industry is taking responsibility for protecting goods and shipments from being misused for such an event. A customs strategy that targets only the ports with screening and scanning controls introduces inefficiencies at these critical points in the transport chain and is at the same time limited in its effectiveness to make supply chain more secure. Regulatory security initiatives, then, are pushing requirements for security measures upstream from the ports and requiring participation of all actors in the supply chain. This means, however, that the logistic systems beyond the ports need to be equally

secured in order to guarantee security of the entire supply chain. The heightened transparency and coordination between the agents operating in the transport of goods and materials that security regulations require have provided supply chains with opportunities to make their processes tighter and more efficient, to examine partnerships with suppliers and customers, and to make the supply chains less vulnerable. Security measures involve procedural changes in operations as well as investments into technology, human resources, compliance with security initiatives, and standardization and communication of security procedures. Supply chain security has consequently come to have strategic importance.

This thesis will first create a framework for analysing security measures using the theory of supply chain management as a starting point. In this way, the groundwork is laid for finding means to make the supply chain both more secure as well as more efficient by looking at principles of supply chain management that can be applied to security improvements. This is the topic of the following chapter.

Chapter 3 Theoretical Aspects of Supply Chain Security

The last chapter looked at the political and economic aspects surrounding the topic of security, including the perceived conflict between the political goals behind the security rules and the economic impact of the security initiatives. Some of the potential costs and impacts of security measures were explored. Security was found to offer a portfolio of benefits for supply chains in achieving higher levels of efficiency and effectiveness as well in making supply chains more secure. The question that arises is how these benefits can be achieved within a supply chain. This chapter sets up a supply chain management theoretical framework for the discussion of supply chain security.

Supply chain management is a means to make the integrated processes and cross-organizational functions of international logistics more efficient. SCM as a theory is considered in terms of its contributions to understanding inter-organizational integration of planning and operational functions in meeting consumer demands through the formation of supply chains. SCM also provides a means of analysing the design and organization of supply chains and logistics networks in order to lower costs, and provide approaches for improving their operational effectiveness.

The issues raised by adherence to security rules relate to how security regulations impede the efficiency of supply chain processes, such as through additional costs and unplanned delays due to security inspections. To overcome the impact of these costs, real gains in operational and strategic efficiency and effectiveness are sought through SCM principles. Efficiency also arises in discussions on logistics and supply chain security as SCS can serve a means to further the inter-organizational integration of business activities along the supply chain. Security also relates to the achievement of competitive advantages related to a supply chain's value creation strategy (Rice 2007).

Another issue within the topic of supply chain security is the ability of a supply chain to respond to unforeseen disastrous events. The event of a terrorist attack would severely test the resiliency of supply chains, as was already seen in the aftermath of 9/11; therefore, steps need to be taken that make supply chains more secure against terrorism, theft, losses and tampering (Baldini, Oliveri et al. 2012). Supply chains must also have the capabilities

to respond to and recover from a disaster given its occurrence in order to limit its impact and facilitate business continuity.

This chapter provides a more detailed background on the theory of supply chain management. It explores the problem of security in the context of supply chain management theory. The operational processes of transportation and storage are extracted from the managerial supply chain activities into a model of a transport chain. Three central challenges posed by security issues are looked at in this framework: (1) creating organizational and procedural efficiencies out of investments into supply chain security, (2) managing security risks, and (3) establishing measures for business continuity. The analysis considers these issues in supply chain security using concepts and terms that have already been given attention by research due their inherence and importance to supply chains: risk, resilience, and flexibility. An overview of the literature on supply chain security is given, which looks at the theoretical contributions of various frameworks to the problem of improving the security of supply chains. Implications of the findings from the literature on dealing with terrorist threats are then found to support the operational decision making in the transport chain. The chapter concludes with a synthesis of the issues central to the topic of supply chain security, a definition of security for supply chains, and a synopsis of issues requiring strategic and operational planning for improving supply chain security, and how security impacts decision making, specifically for the planning of logistics operations.

3.1 Supply Chain Management

Supply chain management is a relatively newer stream of management theory, but an important one, as it offers a means to analyse and manage systems of production and distribution of goods in a post-industrial, highly dynamic, and globally-linked society (Svensson 2004). The last several decades have seen major shifts and innovations in the way goods are produced and distributed (Stonebraker and Afifi 2004), and these changes are major drivers of national and international economies. Supply chains are responsible for satisfying consumer demands for products by bringing them to market at an accelerated pace and at affordable prices (New 1997, Ketchen and Hult 2007). The growth

of consumer markets in (rapidly) developing nations "will make sourcing and supply chains truly global in order to satisfy this demand" (cited by Hameri and Hintsa 2009). And, as markets continue to emerge and grow in developing nations and competition for resources grows, supply chains will have to deal with collecting goods back from the end-users for re-use as input for production. The efficiency of supply chains, then, is directly linked to economic growth and well-being, because supply chain processes govern the production and distribution of goods and services.

The study of supply chains looks directly at how these have emerged and how they can be made to work more efficiently. Figure 3.1 portrays the supply chain across multiple organizations, with the goal of satisfying consumer demand. In such a system, sourcing and manufacturing processes and logistics activities are not only aligned in order to match supply to consumer demand (Hendricks and Singhal 2003), but are also integrated across organizations in order to achieve a higher degree of efficiency and competitiveness, which is not easily imitated (Mentzer, DeWitt et al. 2001, Tan 2001, Ketchen and Hult 2007, Stadtler 2008).

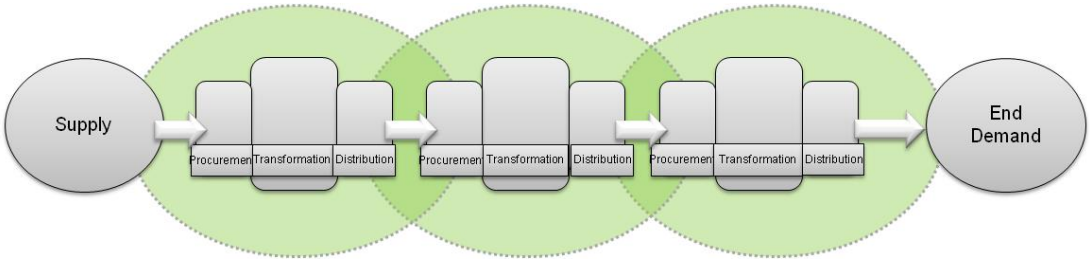

Figure 3.1 Value Creation in the Supply Chain (source: by the author)

The evolution of the supply chain has been driven by several major factors. Globalization of trade and supply chains is a mega-trend resulting in global markets, global products and global manufacturing (Hameri and Hintsa 2009). As a result, competition occurs on a global, rather than a local or regional scale, and the minimal levels of performance required in order to compete have risen accordingly. Companies are therefore increasingly focussed on their own core competencies, whereby they are required to buy assets, services and access to resources from other companies, creating high levels of interdependence in value creation between specialized organizations (Svensson 2004, Hauge, Boschian et al. 2009). In other words, vertical disintegration of

production and materials transformation processes within corporations has co-evolved with horizontal coordination between corporations (Stonebraker and Afifi 2004). The quality revolution is another driving factor, leading companies to seek strategic partnerships with their suppliers in order to be able to influence and control the quality of its products from an earlier point in the production cycle (Tan 2001). Dynamics and uncertainty in the environment also drive developments in supply chains. Fluctuations in consumer demand regarding quantity and quality of products and services, shorter product life-cycles and a high level of innovation leading to new technologies characterize the uncertainty in the environment. Consequently, the level of integration and partnership between organizations dictates the level of quality and competitiveness that can be achieved by a supply chain, in its ability to respond to environmental uncertainties. Figure 3.2 depicts the difficulties in matching the activities of the supply chain to changing demands and in the face of uncertainties: uncertainties in supply markets, uncertainties due to changing technologies and processes and in demand (Chen and Paulraj 2004, Jüttner 2005), in addition to dynamics arising from the environment (Hintsa, Gutierrez et al. 2009).[5] All of these dynamics represent sources of risk for supply chains (Peck 2005, Manuj and Mentzer 2008).

[5] Not all dynamic forces and perturbations are equally valued or disruptive to the supply chain. Hameri and Hintsa, for example, found that supply disruptions presented greater risks than disruptions in demand (Hameri, A.-P. and J. Hintsa ibid."Assessing the drivers of change for cross-border supply chains." (9): 741 - 761.). And the risk of supply disruptions is growing: “Increasingly, major end of supply chain firms, in the form of large retailers and major manufacturers, have so much buying power that their first and second tier supply base is continuing to weaken financially. With the trend of supplier rationalization, this places the buying company at increasing supply risk” (Cavinato, J. L. (2004). "Supply chain logistics risks: From the back room to the board room." Ibid. **34**(5): 383 - 387.). A supply chain’s environment, however, was found to present the most important risks in a study by Manuj and Mentzer (Manuj, I. and J. T. Mentzer (2008). "Global supply chain risk management strategies." Ibid. **38**(3): 192 - 223..

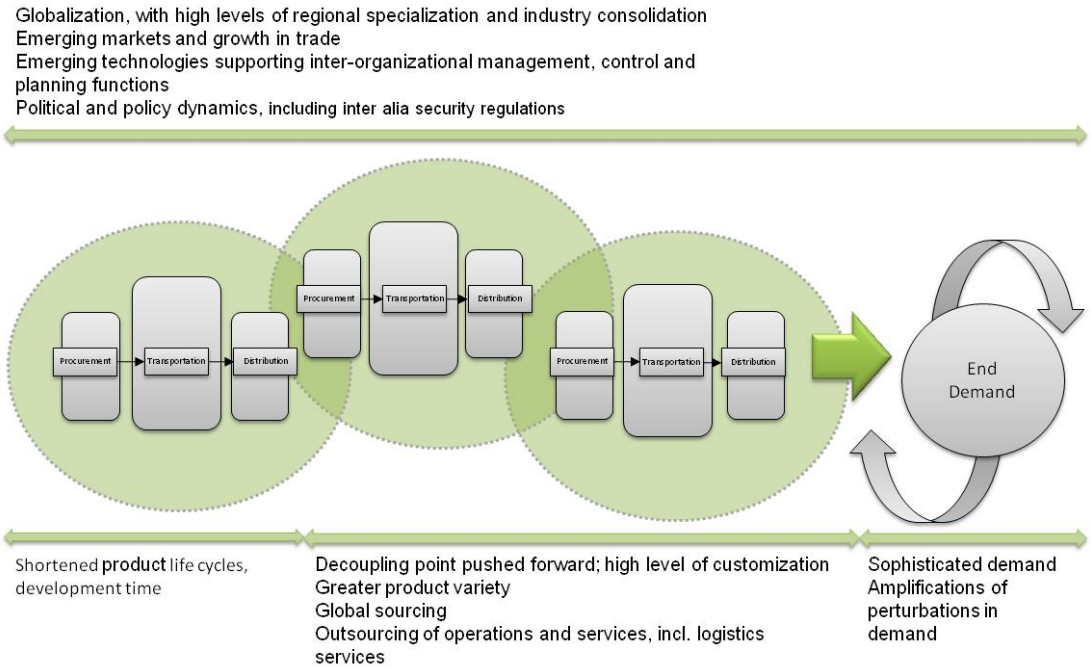

Figure 3.2 Dynamics and Supply Chain Responsiveness (source: by the author)

Despite the relatively recent focus on supply chains in managerial research, supply chain management draws from established knowledge in various streams in the study of management and economics, especially industrial economics, systems dynamics, marketing, purchasing, logistics and transportation, and organizational theory (Croom, Romano et al. 2000, Chen and Paulraj 2004, Ketchen and Hult 2007). SCM offers concepts, principles, approaches and methodologies to reduce costs and improve the effectiveness of business activities (Svensson 2003). Operationally, supply chain performance can be measured in terms of efficiency, reliability and responsiveness (Hendricks and Singhal 2003). Supply chain management in this context concerns itself with the optimization of the flows of material, goods and information at the inter-organizational level (Haasis 2008).

In order to improve business processes, and because of the interdependencies between organizations, supply chain management deals with relationships between organizations that govern the processing and flows of materials, goods and information. The unit of analysis in SCM is, then, the dyadic buyer-supplier relationship, in which inter-

organizational integration of business processes happens (Svensson 2004). It is from the perspective of this dyadic relationship that the levels of strategic alignment, sharing of information and collaboration in planning, can be analysed. Moreover, the buyer-supplier relational perspective can be extended across a chain of interdependent organizations as well as across a network. From this perspective, value is created not within a single company, but by a chain or network of strategically aligned firms (New 1997, Ketchen and Hult 2007).

Where satisfaction of consumer demand, referred to from now on as *value creation*, is the ultimate driver of supply chain management, new methods have evolved that allow supply chains to respond to increasingly sophisticated consumer demand with higher levels of availability, responsiveness and customization.[6] These approaches require a tighter alignment between companies in the form of coordination or process integration (Stadtler 2008). In general, supply chain management approaches, such as Just-in-time, Quick Response, or Total Quality Management, require integration and coordination between organizations. Here integration refers to actions aimed at aligning supply chain management practices to a company's goals to achieve improved performance and efficiency (Mentzer 1991, Stadtler 2008, Lintukangas, Peltola et al. 2009). This level of coordination can only be achieved with extensive information sharing, which is possible only in trusting relationships (Akkermans, Bogerd et al. 2004). From this we can see that integration of business processes involves information, coordination and cross-organizational relationships (Stock, Greis et al. 2000). One of the tenets of SCM, then, posits that having a smaller number of more strategic suppliers or partners provides a basis for improving quality of products, flexibility and reaction time, and overall efficiency (Chen and Paulraj 2004). The end-objective of such an integrative strategy is a long-term competitive advantage (Hendricks and Singhal 2003, Ketchen and Hult 2007). Figure 3.3 shows the dynamics influencing logistics and supply chains and the inter-organizational management competencies required to deal effectively with these dynamics.

[6] "It is the development of values among end-customers which will direct consumption and those companies that best comply with these trends will be the future winners" Hameri, A.-P. and J. Hintsa (2009). "Assessing the drivers of change for cross-border supply chains." Ibid. **39**(9): 741 - 761..

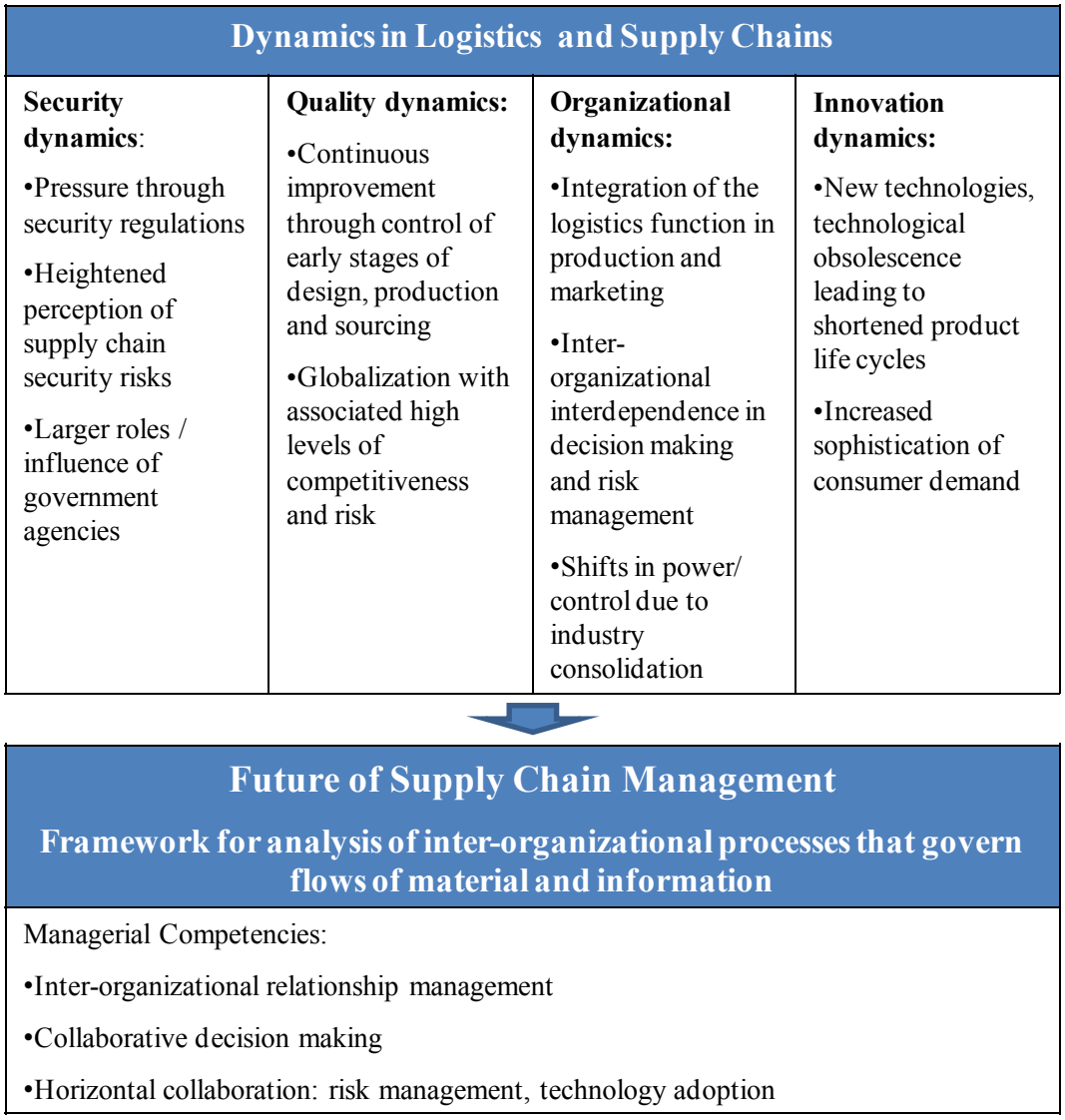

Figure 3.3 Dynamics in Logistics and SCM and Areas for Future SCM Development and Research (source: by the author)

While manufacturing and planning processes are being aligned between actors in a supply chain, the logistics functions have also come be integrated in a broader supply chain strategy. It was already stated that logistics and transport studies have been incorporated into the development of supply chain management. The manufacturing processes along a supply chain are increasingly coupled with sourcing and distribution strategies, which include inventory, warehousing, distribution and transportation planning.

As the planning windows for these processes become shorter, inventories become smaller and transportation management becomes more critical (Esper and Williams 2003). Going forward, it is expected that the logistics function will be integrated to a greater degree in the supply chain, not only surrounding the procurement, manufacturing, and distribution processes, but also as early as the product design stage.

Another development in the logistics function in terms of transportation and warehousing is the high degree of outsourcing. Where logistics is considered to be movement (of goods) over time and space (Sheffi 1985), costs rise as a function of the time spent in inventory, and distance travelled. A major concern historically has been the cost structure of logistics flows, whereby the cost per unit is lower as the flows become larger, consequently leading to greater consolidation. Consolidation of shipments lowers total costs in both transportation and warehousing due to these economies of scale. Multiple commodities complicate consolidation in all areas of logistics; for this reason, economies of scale can be achieved best by firms specializing in logistics services. This has led many companies to outsource these functions to logistics service providers who can perform these functions more efficiently (Bottani and Rizzi 2006). Operational performance of third-party logistics service providers (LSPs), then, rises in strategic importance and requires a greater deal of collaborative effort.

To illustrate the separation of supply chain operations from logistics activities, a transport chain as a parallel chain of operations to the supply chain can be introduced (compare New and Payne 1995), as is depicted in Figure 3.4:

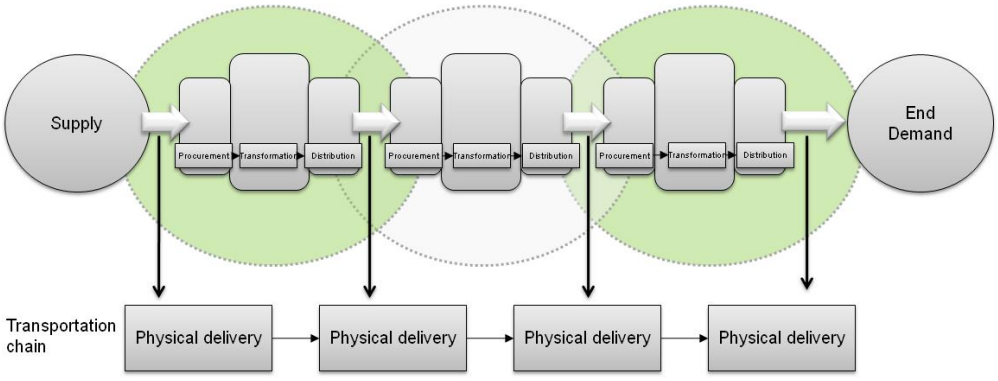

Figure 3.4 Transport Chain (source: by the author)

A picture of the transport chain as a separate and distinct unit of analysis is helpful because it more closely reflects the interdependencies and distinctness of interactions that happen between supply chain partners and logistics service providers, and it highlights the decision structures between the supply chain, the transport chain, and their surrounding environment. Separating the operational level from the managerial level also allows one to look at several implications for the supply chain, specifically in the area of security, related to the integration of the logistics function along the supply chain and the outsourcing of this function to logistics services providers.

The first implication of outsourcing the logistics function is that LSPs act as integral partners in achieving strategic goals (Bottani and Rizzi 2006), where the physical transportation and storage of materials required at any point in the supply chain is determined by the supply chain strategy. Size of consignments, flexibility in their availability and allowable lead times, cost limitations and trade-offs of increased costs to supply chain flexibility and responsiveness are all points that will determine the configuration of the material flow. Requirements for postponement in manufacturing, for example, will mean less flexibility will be allowed in the logistics process due to shorter time buffers. Hence, decisions on the operational level are largely dictated by the supply chain design at the strategic.

Second, the tightening of alignment between companies means that slack in the form of lead times and inventory are minimized; reliability of logistics services is then necessarily the foremost requirement in their delivery. Any disruptions in the delivery of goods, especially unexpected delays or losses through theft or damage, in the transportation chain will inevitably introduce extra costs into the supply chain and reduce the value of the outcome of supply chain activities.

Third, outsourcing the logistics functions comes with the expectation of cost savings, which in turn puts several cost restrictions on the logistics service providers. LSPs consequently work under conditions of slim profit margins in a highly competitive environment. Finally, outsourcing of the transportation and warehouse functions means that the physical movement and storage of materials and goods is performed by actors who have custody, but not ownership of the goods they are carrying, and in some cases, do

not even know what goods they are carrying. Not only that, but a lack of transparency in the logistics function appears at the supply chain level as a "black hole" into which the goods "disappear", until they reappear at the other end, as these functions are outsourced (Sheffi 2001).

All of these implications factor into the operational effectiveness of supply chain strategies as well and into the security of the physical movement and storage of goods.

3.2 Supply Chain Security: Problems and Definitions

The topic of security has received increased attention in recent years in supply chain management literature. The problems of increased pressure on the logistics industry to increase their security programmes and adhere to security regulations, and the costs of such programmes are threats to the efficiency of supply chains, as was described in Chapter 2. At the same time, supply chains face security risks including theft and the threat of terrorism and smuggling involving transports. These risks threaten business continuity and financial performance. In order to identify the state-of-the-art of the research on supply chain security, a literature review was performed.

A structured literature review of a topic is generally used to delineate the research area by identifying the scope of the issues dealt with in a given research topic, and understanding what methods exist for dealing with these problems, as well as the strengths and weakness of the applied methods (Boote and Beile 2005). As one method for reviewing the literature, a content analysis was undertaken for the literature on security in supply chains. Articles on supply chain security were collected and classified according to instrumental categories (Marasco 2008). Commonly used academic sites including Emerald Insight, Science Direct, two EBSCO databases Business Source Premier and EconLit, and Wiso-Lit were searched. This last database accesses German-language sources, including business and economics journals over several searchable databases, including: BLISS, Econis, FinEcon, ifo Katalog, ifo Publikationen, IHS Literatur, Kölner (Business) Katalog, and MIND Kreditwissenschaftliche Literatur. The terms "supply chain security" and "logistics security" were used for searching and, due to the newness of the research area, additional search terms including "vulnerability" and "risk" were used

to include a broader collection of articles. Articles were found from as early as 2000 up to an including publications from 2012. Publications from journals, magazines or periodicals not directly considered related to business management or economics were excluded. Moreover, articles were excluded that deal with related but not included issues. The excluded articles touched on the issues of: losses and damage through packaging; road safety; providers of security solutions; security of persons in a social/civilian sense, and security of data/information.

The collected literature on supply chain security revealed several categories of issues. Table 3.1 gives an outline of the different areas of supply chain security discussed in the literature:

Table 3.1 Generalization of Issues and Problem Areas

Problem Area	Articles
SC Efficiency in the context of Security Requirements	
Understanding the impact of certification and/or adherence to security regulations in a supply chain	(Kern 2007), (Neumann 2008),(Fletcher 2007), (Hameri and Hintsa 2009), (Macpherson and McConnell 2007), (Banomyong 2005), (Yang 2011)
Potential or incurred benefits of security measures and programmes	(Logistik Heute 2008), (Wieland 2008),(Fletcher 2007), (Peleg-Gillai, Bhat et al. 2006), (Crutch 2006), (Voss, Closs et al. 2009), (Bichou, Kee-Hung et al. 2007), (Thai 2009)
Drivers and strategic relevance of security programs	(Whipple, Voss et al. 2009), (Hameri and Hintsa 2009), (Vance 2008), (Williams, Lueg et al. 2008)
Dealing with Security Risks in Supply Chains	
Interdiction of terrorism involving transport	(Haag 2007),(Williams, Lueg et al. 2009)
Reducing losses due to theft/damage	(Neumann 2008), (Kempf 2008),(Logistik Heute 2005),(Weise 2005),(Fischer 2005)
Understanding and reducing vulnerabilities and security risks in supply chains (terrorism, theft, information security risks, counterfeit risks, etc.)	(Kotsiwos 2008),(Müller 2008), (Chopra and Sodhi 2004), (Knemeyer, Zinn et al. 2008), (Cavinato 2004), (Laeequddin, Sardana et al. 2009), (Wagner and Bode 2006), (Bandyopadhyay, Jacob et al. 2010), (Cozzella, Simonetti et al. 2012),

	(Enyinda and Tolliver 2009), (Kerschbaum, Schröpfer et al. 2011). (Kumar, Jensen et al. 2008), (Kumar and Verruso 2008)
Strategic decision making for security in supply chains	(Badea, Rocco S et al. 2011)
Improving Response to a Security Event	
Recovery from an incident	(Hale and Moberg 2005),(Baldini, Oliveri et al. 2012)

Three major objectives exist for investing in supply chain security: heightening security of supply chains, improving efficiency of business processes, and improving response and resilience to security incidents (Gutiérrez, Hintsa et al. 2007).

In order to meet the objective of making supply chains more secure by overcoming vulnerabilities, both organizational methodologies, such as risk management and quality management approaches, and technological approaches, including applications of visibility technologies such as Track & Trace and information security can be applied. Security threats in this context include vulnerabilities to: theft, loss, sabotage, information security risk, and counterfeit risks.

The second major objective is that of improving business processes, specifically in the context of security requirements. In the earliest papers on SCS the focus was on compliance with regulatory security initiatives as a means of avoiding delays at border crossings and in customs processes, as well as against the impact of a security event, such as closed borders, a port shut-down or a loss in image. Public-private partnerships are a key phrase in this context (IBM 2004). Here security measures are now considered as a cost of doing business in the post 9/11 environment, and drive the requirement to achieve benefits for these costs, which are mostly sought in efficiencies in supply chains, including smoother border crossing. The research towards this objective aims at fixing guidelines for implementing structural changes to business processes along supply chains to make them more efficient. Research directions in this area include a look into industry leaders of SCS, understanding the impact of security initiatives, and looking for ways to benefit from compliance.

The third major objective in implementing security measures is to improve the ability of the supply chain to detect and react to security incidents (Voss, Whipple et al. 2009), or, in other words, to improve resilience and response capabilities – agility and flexibility (Baldini, Oliveri et al. 2012) - to a security incident or a disaster. The length of time to respond to the event is correlated to the volume of impact that the disaster will have. It is therefore important to respond to a security event quickly.

Towards these objectives, strategic decision making and decision support are only very recently coming to the fore in the literature. Badea et al. (2011) use Group Decision Theory to derive composite indicators for energy supply security to support policy decisions.

Prior to 2007, security was used persistently as a term in the literature, but was most often left undefined (Gould 2007). In the context of the threat of terrorism, "security" refers to a general sense of well-being, and a confidence in the continuity of the present - especially business - conditions. On the other hand, "security" is also used to refer to any modifications made to supply chain processes, both organizational and technical, that are taken to prevent undesired events from taking place, such as theft, terrorism, crime, or sabotage. For security programmes, the ISO 28000: 2007 defines supply chain security as "resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain" (ISO 2007). Risk prevention aspects are also taken into account in the definitions given in recent publications by Closs et al. (Closs, Jacobs et al. 2008), Whipple et al. (2009), IBM's reports (Crutch 2006, Fletcher 2007). Table 3.2 provides an overview of definitions of SCS found in the literature.

Table 3.2 Definitions of Supply Chain Security

Conceptual Definition	Articles
"SCS management covers all processes, technologies and resources exploited in a systematic way to fight against end-to-end supply chain crime; the primary goal of each single SCS measure is either to prevent a crime, to detect a crime, or to recover from a crime incident in the fastest possible time; single SCS measures fall typically within one of the following five categories: cargo, facility, human resources, information technology, and business network; the typical	(Hintsa, Gutierrez et al. 2009)

supply chain crime includes theft, smuggling, counterfeiting, sabotage, blackmailing for financial gain, terrorism for destruction, and any type of fraud and corruption (the detailed crime definitions subject to national and international regulations)."	
"Within IBM, supply chain security is defined as protecting products, facilities, equipment, information, and personnel from theft, damage, or terrorism, and preventing the introduction into the supply chain of unauthorised people, contraband, or weapons of mass destruction or effect. Such weapons, for example, are capable of inflicting grave destructive, psychological and/or economic damage, and include chemical, biological, nuclear, radiological, or explosive weapons."	(Fletcher 2007)
"Supply chain security management is the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction/effect into the supply chain."	(Crutch 2006), (Kumar, Jensen et al. 2008)
"The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism and to prevent the introduction or unauthorized contraband, people or weapons of mass destruction into the supply chain (Closs and McGarrell, 2004, p. 8)."	(Williams, Lueg et al. 2009), (Voss, Closs et al. 2009), (Whipple, Voss et al. 2009), (Williams, Lueg et al. 2008)

The above-listed definitions of supply chain security highlight the human aspects of the perceived risk. The topic of security in supply chain management currently deals with the prevention of the risk of man-made disasters (Williams, Lueg et al. 2009), including the elements of terrorism, biological warfare and chemical warfare, smuggling and contraband, fraud, etc. Security threats, or risks, to supply chains dealt with in the literature can be categorized into several major areas: 1) the threat of a container or a transport being used for criminal purposes; 2) inefficiencies in the supply chains because of regulations and security initiatives; and 3) costs of disruptions in the flow of goods and services. Developments in SCS literature also include security of energy supply (Badea, Rocco S et al. 2011) and information security in inter-organizational supply chains (Bandyopadhyay, Jacob et al. 2010, Kerschbaum, Schröpfer et al. 2011).

The literature on terrorism risks involving the transportation industry deals with the threat of criminal interception or misuse of transports. In the past, legitimate commercial shipments were tampered with, and used to transport contraband, even illegal persons (Lee 2004). The threat includes the risk that a container might be used to transport a weapon of mass destruction (WMD). A further risk is of a shipment of hazardous goods (HAZMAT) to be misguided and used as a means of an attack. Government-led security regulations focus on prevention, and aim to reduce the possibility of a terrorist attack taking place (Willis and Oritz 2004, Lake, Robinson et al. 2005), by reducing any possibility unauthorized access to the transport containers or shipments, and making the supply chain more transparent. These security measures in general require investments into personnel, technology, security planning, physical facility security, as well as investments relating to regulatory compliance. At the same time, compliance alone can only be a cost factor, rather than a means to improve processes and create efficiencies, and represents the second category of threat to the supply chain. The research on this aspect of supply chain security focuses often on cost-benefit analyses of employing new technology, and potential areas of improving efficiency of operations, i.e., through better information-sharing between strategic supply chain partners.

The cost of disruptions in the globalized transportation industry is potentially very high, and therefore has raised the issue of vulnerability of supply chains to disruption. The concept of vulnerability in supply chains is central to the discussion of supply chain security. Vulnerabilities refer to any weaknesses in a supply chain that make it susceptible to loss due to a security event (Barnes and Oloruntoba 2005, Wagner and Bode 2006). Vulnerability represents not only the possibility of an undesired event taking place, or of an attack bypassing security measures and precautions, but also the extent of the impact the event would have. It was pointed out that the characteristics of the transport system result in several vulnerabilities, especially the complexity, volume and lack of transparency in the logistics sector; the interconnectedness within the transport industry; and the lack of redundancy (Transportation Research Board 2002, Barnes and Oloruntoba 2005). Supply chain management practices are themselves vulnerable (Jüttner 2005).

Moreover, lacking visibility is a cause of concern in supply chains and one that makes dealing with vulnerabilities difficult (Francis 2008).

It is well recognized that security for a supply chain is beyond any single firm, but rather demands attention to the entire process, where vulnerability at any point represents a weakness downstream. This has moved the concept of supply chain security beyond isolated measures such as closed-circuit television or physical access controls. The approach to improving security of supply chains is seen instead as an organizational problem, where vulnerabilities are created by the design and processes inherent to the supply chain itself, especially in the inter-organizational interfaces. In this case improving the security situation requires an analysis of the supply chain, the actors within it, their interfaces, and the processes involved, including facilitating technologies.

3.3 Theoretical Approaches to Supply Chain Security

3.3.1 Supply Chain Risk Management

Risks are recognisably inherent to supply chains, but the terrorist attacks of September 11, 2001 and in the subway systems in London and Madrid in 2004 have arguably broadened the definition of risk and perceived sources of uncertainty to include the risk of manmade disaster (Cavinato 2004). Managing risk involves identifying risks, assessing risks, and finding a management strategy to deal with the risks whose impact is deemed too great using mitigating strategies. Once a risk, or hazard, is identified, the risk is quantified using a likelihood of occurrence and a probabilistic impact, such that risk is calculated as the product of the probability of an incident occurring and its consequence (Manuj and Mentzer 2008).[7] [8]

[7] This negative-sided description of risk relates only to the potential losses of an event, and does not consider any positive outcomes or opportunities created by the event, as is used more frequently in financial risk management. Compare understanding of risk from Peck, H. (2005). "Drivers of supply chain vulnerability: an integrated framework." Ibid. **35**(4): 210-232..

[8] Manuj and Mentzer added two additional dimensions to risk: speed of risk impact occurring, of its consequences, and its detection; and frequency of the incident occurring. The authors write, “Speed and frequency together determine the losses that happen per unit of time” Manuj, I. and J. T. Mentzer (2008). "Global supply chain risk management strategies." Ibid. **38**(3): 192 - 223..

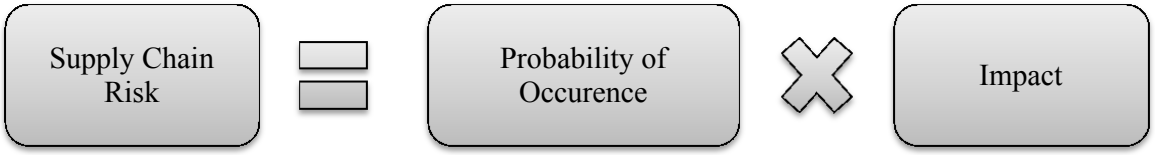

Figure 3.5 Calculation of Risk in Supply Chains

The goal of risk management (RM) is to guide decisions for investment and process analysis to either reduce the likelihood of an undesirable incident occurring, or reduce its impact, and is applicable for dealing with security risks in the supply chain. An RM methodology is applied, for example, by Tzannatos (2003) for the creation of a decision support system for shipping security. Risk management approaches also form the basis of the security measures proposed by the US-led C-TPAT, CSI and 24-Hour rule, as well as the ISPS Code, for which a security risk profile resulting from a risk assessment is the key to its effectiveness (Thai 2009). These sets of security measures propose that only a small number of containers pose any security threat, and security measures must be applied sensibly and target only high-risk containers. In order to identify errant containers, the security measures attempt to raise the level of transparency[9] in shipping by creating programmes for early forwarding of documentation,[10] automatic identification of containers and ships, and a registry of approved compliant shippers and logistics service providers. In this way, routine shipments by participants in the programmes are kept from receiving additional scrutiny.

The very low probability of a terrorist attack associated with any given container shipment leads to low-risk priority placement from a risk management perspective. In contrast, supply chains are more adept at dealing with high-probability risks (Chopra and Sodhi 2004, Knemeyer, Zinn et al. 2008). From a theoretical standpoint, risk-averse managers may tend towards risk avoidance in such cases (Erkut and Ingolfsson 2000, Knemeyer, Zinn et al. 2008), but not mitigation, which is what is required by regulatory

[9] Shipment transparency was defined as its legitimate representation to authorities and its legality Willis, H. H. and D. S. Oritz (2004). Evaluating the Security of the Global Containerized Supply Chain. RAND Corporation. Santa Monica, CA..

[10] Delays in information flows cause congestions and insufficient delivery reliability Plöger, M. and H.-D. Haasis (2009). Overcoming information integration barriers in multi-tier supply chains with programmable RFID devices, Institute of Shipping Economics and Logistics (ISL)..

security measures. Despite this general risk behaviour, more attention is being drawn to risk management as a means to deal with catastrophic risks in supply chains, including the threat of terrorism (Cavinato 2004, Chopra and Sodhi 2004), because of the potential magnitude of the impact of terrorism, as well as other high-impact disturbances, on supply chains. A new direction for supply chain risk management towards low-probability high-consequence (HP/LC) problems has therefore emerged.

Due to the importance of security risk to the modern supply chain, such risk requires the attention of executive management and their direction in broadening the scope of risk management processes (Cavinato 2004). Security/control systems were posited as a means of reducing supply chain risk in general by Laeequddin et al (2009), and Manuj and Mentzer suggested using security to guard against demand and supply risk specifically (Manuj and Mentzer 2008). The extended possibilities for mitigating security risks are largely organizational in nature, relying heavily on inter-organizational and public-private partnerships. Risk management, then, begins to have a supply chain approach rather than a firm-driven approach.

RM, its relationship to SCM in the literature, and areas for future research are discussed by Peck (2006) and Jüttner (2005). Outlining the risk in supply chains, Peck (2005) illustrates the interdependencies between the procedural, structural, and organizational layers of the supply chain, as shown in Figure 3.6:

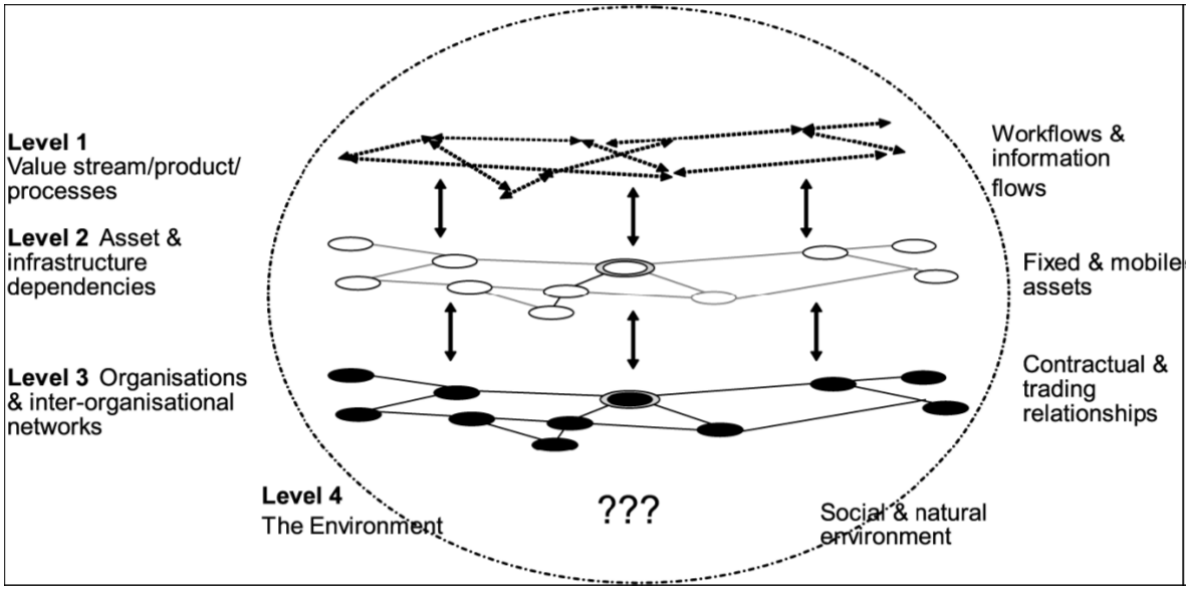

Figure 3.6 An integrated model of a supply chain (Peck 2005)

Peck's work points out that risks and disturbances at the level of assets and infrastructure and that of the inter-organizational network as well as in the social and natural environment impact the supply chain at the value stream level. One finding is that risks are not only inherent to supply chain processes, but are exacerbated by methods designed to make these processes more efficient by means of reducing redundancies and buffers (Chopra and Sodhi 2004, Knemeyer, Zinn et al. 2008), including lean manufacturing and increasing integration (Norrman and Jansson 2004). Another finding is a general lack of the transparency along supply chains required to understand risk sources and potential impacts, communicate plans for risk mitigation, and share the burden of risk mitigation (Jüttner 2005). Norrman and Lindroth define supply chain risk management (SCRM) as " 'collaboration' with partners in a supply chain risk management process…to deal with risks and uncertainties caused by, or impacting on, logistics related activities or resources" (Norrman and Jansson 2004). Consequently there is a strong requirement in supply chain management for RM for the purposes of identifying, assessing and mitigating risks (Kumar, Jensen et al. 2008).

The RM framework allows us to understand the nature of the impacts of catastrophic events on supply chains as interruptions on workflows and information flows at the

procedural level. In response to this problem, Knemeyer et al. research ways to assess the risk of terrorism and other catastrophes by calculating probabilities of occurrence and impact of such incidents in order to help managers understand risks and make decisions towards mitigation strategies (Knemeyer, Zinn et al. 2008). This method allows for a quantitative assessment of both probabilities of uncertain events, as well as the impact of their occurrence, and therefore takes advantage of one of the advantages of RM approach in facilitating a quantitative assessment for a cost-benefit analysis for investments.

Research until now has focused on making the supply chain less vulnerable to a terrorist attack firstly by gaining a deeper understanding of security risk, specifically that of manmade disaster. The potentially high impact of these risks is an impetus for a risk management area that has emerged to deal more specifically with low-probability/high impact risks. The literature so far, however, has not supplied evidence linking security practice to either improvements in security - in heightened detection of incidents, better response to incidents, etc. – or to improvements in performance, in terms of delivering better quality or customer service (Whipple, Voss et al. 2009). Normann and Jansson (2004) further posit that there is still a lack of understanding of how to identify and assess trade-offs between risk management practices and principles of supply chain management to achieve efficiency. So, while SCRM might offer insight into the application of RM for dealing with the risk of terrorism in supply chains, the problem of quantifying a cost-security trade-off still persists (Kumar, Jensen et al. 2008).

3.3.2 Quality Management

Quality management provides insight into how supply chain processes can be improved to make them less vulnerable by eliminating non-desirable factors. For one thing, QM focuses on problem prevention. For another, QM offers guidelines for reducing costs through relationship with suppliers. Lastly, QM offers a means to strive for a competitive advantage through satisfaction of customer demand. There are limitations of its application to solve problems of supply chain security, however, due its internal focus on processes, which contrasts with the external sources of security risk. Another general problem relates to the use of certification as a tool to demonstrate adherence to quality

standards without any substantial changes that would, in fact, raise the security of processes and shipments.

Quality management methods were applied to logistics processes before supply chain management became an established research field in management theory. Quality management provides methods for analysis and performance measures of processes to find areas where quality variations are created, rather than attempting to identify non-compliant finished products. In other words, QM focuses on problem prevention, source inspection, process controls and continuous improvement (Thai 2009, Hintsa 2010). In this way, control of deviations from the expected, or integrity, is the aim of international security initiatives (OECD 2005). A QM approach to logistics security translates into ensuring the integrity of a shipment from the point of origin through the supply chain (Sheu, Lee et al. 2006). Lee and Whang (Lee and Whang 2003) argue that the application of QM can improve both the cost efficiency and the security of supply chains by improving relationships with suppliers. Bichou et al. demonstrate how QM can be used by liner shipping companies to meet regulations, while allowing them to meet service and cost goals to reach a competitive advantage (Bichou, Kee-Hung et al. 2007). The applicability of methods from quality management to supply chains is due to its cross-functional approach with a focus on satisfying customer demands (Beamon and Ware 1998), an objective it shares with SCM, as well as seeking the backing of executive support (Thai 2009).

QM's focus on internal risks as departures from a standardized norm is one limitation of the theory's applicability for supply chain security problems, as it lacks the ability to deal with risks that persist due to non-controllable hazards from outside of the managerial scope. The risk of terrorism belongs to this category of risk, such as criminals learning to avoid precautions (Hintsa 2010).

Another overarching limitation is related to the general critique of implementing quality management, such as that given by Sroufe and Curkovic (2008). In their study of applications of ISO 9000:2000, the authors showed that there are ambivalent benefits and improvements to quality from adherence to the quality management standards. If supply chains adopt security measures the same way that QM measures are adopted, there may or

may not necessarily be measurable improvements to the vulnerability of a supply chain (Hintsa 2010). Moreover, "emphasis on the demonstrated compliance to the standard for suppliers has led some businesses to seek registration only in order to win customers or remain on 'approved supplier lists'" (Sroufe and Curkovic 2008). Not only that, some companies are seeking certification only because of pressure by existing customers. This is specifically a problem with smaller organizations. This problem resembles what has been the case with certification according to security measures.

It was also pointed out that there is a lack of research on strategic frameworks and quality management (Sroufe and Curkovic 2008). Sroufe and Curkovic asserted in their study of security guidelines that, while certification along security regimes is useful for analysing the security situation of the supply chain and implementing security measures, certification has limited usefulness in creating a managerial security concept that encompasses all areas of the supply chain. The authors proposed graduated certification based on security levels to overcome these limitations, which is some ways reflects the implementation of total quality management concepts (Kern 2007). The authors propose the following framework for placing firms with varying competitive strategies (according to competitive typology from Miles and Snow 1978): (Sroufe and Curkovic 2008)

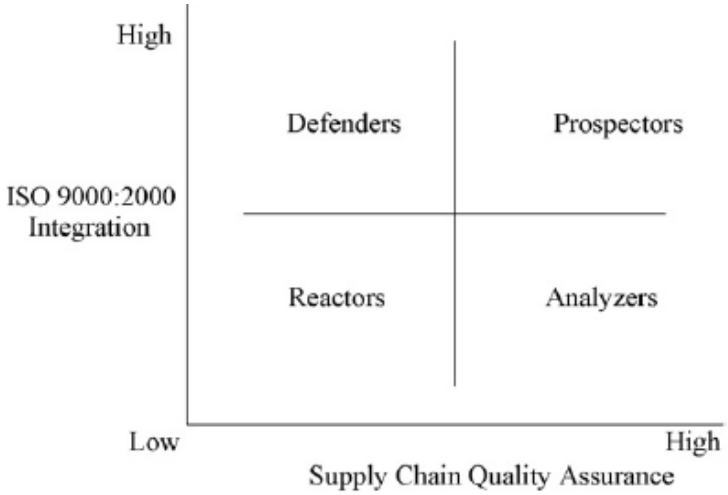

Figure 3.7 ISO Integration and SC Quality Assurance: An Application of Miles and Snow Typology (Sroufe & Curkovic, 2008)

So, in sum, the same problems that have arisen in the area of adherence to security rules and initiatives exist in adherence to quality management standards. Applying quality management principles is helpful, especially regarding prevention and detection of anomalies in supply chain processes (Hintsa 2010); however, the lack of relationship between quality management standards and the strategic direction-taking for competitive strategy mirrors an implementation of security measures that does not benefit from real improvements to processes in achieving strategic goals for security.

3.3.3 Crisis Management

Crisis management is applicable to supply chain security, because it deals specifically with two major concepts central to problems in that research area: vulnerability and resilience. It was applied to logistics security by Barnes and Oloruntoba (2005), who demonstrate that crisis management should be used to helps firms perceive and minimize losses due to a damaging event. Svensson created a construct of corporate vulnerability based on time, relational, and functional dependencies in a supply chain (Svensson 2004), while Wagner and Bode investigated supply chain characteristics that contributed to a supply chain's vulnerability (Wagner and Bode 2006).[11] Vulnerabilities, or security gaps, refer to weaknesses in the supply chain that make it susceptible to an undesired event; vulnerability represents not only the possibility of an undesired event taking place, or of an attack bypassing the security measures, but also the extent of the impact the event would have (Timmerman 1981)[12]. Resilience, then, is the counterpart to vulnerability, and is the ability of a system to recover after a damaging occurrence (Timmerman 1981, Peck 2005). In response to the presence of vulnerabilities, investments need to be made into the adaptability and resilience of the supply chains (Willis and Oritz 2004). There are two

[11] It was pointed out that the own characteristics of the transport system that result in such vulnerabilities, especially the complexity, volume and lack of transparency in the logistics sector; the interconnectedness within the transport industry; and the lack of redundancy Transportation Research Board (2002). Deterrence, protection, and preparation : the new transportation security imperative. Special report. Washington, D.C., Transportation Research Board**:** x, 84 p, Barnes, P. and R. Oloruntoba (2005). "Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management." Journal of International Management **11**(4): 519-540..

[12] Vulnerability was defined as "little strokes that fell great oaks", that is (critical) points (of place or time) of weakness where even small interventions can induce great impact (Abrahamsson, 1997). In contrast, D'Este and Taylor (2003) argue that vulnerability should only be concerned with consequence.

main strategies for achieving resilience: redundancy, and flexibility. Redundancy is the duplication of resources to be used in the case of disruption (Sheffi 2001), whereas flexibility is the ability to adapt quickly. Another important contribution of crisis management is in the necessity of perceiving the development of a crisis, as well as detecting when a crisis has occurred in order to be prepared for it. It is understood that the ability of management to recover from a disturbance is largely determined by the amount of time required to reach resolution; that is, the more time required to deal with a disturbance, the greater the impact. Therefore, firms that have action plans to deal with crises are able to incur less loss as a result of a crisis than firms which have none, even if the crisis was non-predictable. By contrast, firms that do not prepare, "gamble that they will avoid the effects of a disruptive/damaging event" (Autry and Bobbitt, 2008, p. 56).[13]

Crisis management is built on concepts of complexity and looks at the world as an open, complex system in which the organization is a system operating within this system. Because complexity leads to vulnerability, the achievement of the objectives of a system relates directly or indirectly to perturbations in the system or in the environment. For an organization, catastrophic events, such as natural disasters or labour strikes, are recognized in this framework as a threat to business continuity. Catastrophic events are ones over which business managers have no control, but create significant social losses. Managers must instead be able to recognize and respond to disasters in a way that minimizes losses in the long-term.

For supply chains, crisis management is useful in that it draw attention to the vulnerabilities created by the interdependencies of firms, and impacts due to the network nature of supply chains (Svensson 2004). Building on the concepts of vulnerability and resilience, an organization responds to the potential for crisis by first having mechanisms

[13] "The typical large US corporation has given disaster preparedness a low priority because of competing business issues, the lack of recognition of the true level of disaster vulnerability, and an assumption that the service and government sectors are responsible for disaster response. The threat of more terrorist attacks, increasing global unrest, and higher occurrence of major natural disasters creates a powerful motivation for management to explore the processes to secure the performance of the commercial supply chain" Helferich and Cook, 2004 p.2. cited by Hale and Moberg Hale, T. and C. R. Moberg (2005). "Improving supply chain disaster preparedness: A decision process for secure site location." International Journal of Physical Distribution & Logistics Management **35**(3): 195 - 207..

in place to interpret happenings in the environment to foresee catastrophes, and by having programs in contingency plans in place for the event that the catastrophe arises.

3.3.4 Findings from Supply Chain Security Approaches

Applying the frameworks of quality management, crisis management and risk management highlights some requirements for a framework for security, considering the three main aims of implementing security measures framed by Gutiérrez et al. (2007). The following table gives a summary of the contributions drawn from risk management, total quality management, and crisis management for requirements from a framework in achieving supply chain benefits from security measures:

Table 3.3 Requirements of security measures to benefit supply chains (source: by the author)

	Quality Management	Crisis Management	Risk Management
I. Direct Security Benefits	Improve the integrity of shipments and documentation	Understanding the sources of vulnerabilities	Understanding/ assessing risks
II. Business Process Improvements	Increase transparency along the SC Improve supply chain relationships in achieving security standards	Establish plans for business continuity following a security incident	Communicate risk mitigation strategies
III. Reactivity and Resilience	Earlier detection of anomalies	Perceive potential and developing threats and risks in the environment	Mitigate the impacts of security incidents

Looking at these approaches we can generalize several key lessons. First, the security of supply chains is seen as an organizational problem, where risks and vulnerabilities are inherent to the supply chain itself, and are especially prominent in the inter-organizational interfaces. Partnerships are noted to be a key to improving the security of a supply chain, first with suppliers, LSPs, and customers, and also with government bodies; inter-firm relationships and processes can potentially produce efficiencies while meeting requirements for improved security. Collaboration is therefore required for effective security handling at interfaces, considering the processes involved, including facilitating technologies. Secondly, forewarning mechanisms are required including capabilities to understand where threats exist in the environment and how to foresee and forestall a risk is the first step to dealing with it. Moreover, having a response plan in place as well as in the event of a security incident will limit the duration and force of the impact that the security incident will have on the supply chain and its surrounding environment. The aim is to minimize vulnerabilities and build resilience to allow the supply chain to deal with evolving threats and respond to disasters without sacrificing efficiency.

3.4 Categorization of Supply Chain Security Measures

There are some results emerging in the literature for dealing strategically and operationally with the threat of terrorism or security threats in general as well as with the impacts and costs of adherence to security regulations, and there have been proven advantages to business for investing time and resources into supply chain security.[14] The first and most prevalent strategic measure involves creating tighter communication between supply chain partners to plan and control security measures (Autry and Bobbitt 2008), including increased information sharing around transportation flow and potential risks between industry and transportation authorities (Kumar and Verruso 2008). Communication of security processes along supply chains provides a basis for all the other strategies. Preliminary results from analyses of benefits of secure measure point to a tighter level of collaboration and communication with supply chain partners concerning security results in more information sharing (Peleg-Gillai, Bhat et al. 2006), creating more visibility between supply chain partners and potential for making business processes more efficient and secure. Smooth information flows regarding inventory levels, demand levels and current supply is one way promoted in the literature to buffer the supply chain against supply chain disruptions (Martha and Subbakrishna 2002). Wilson, for example, showed that a multi-echelon supply chain employing a vendor-managed inventory replenishment system deviated less in inventory and service levels less than when VMI is not employed (Wilson 2007).

The second strategy is viewing compliance with security regulations as a strategy for security and a means to communicate a firms' action-taking regarding supply chain security with its suppliers and customers. Adherence and certification along international security regulations is especially important for facilitating border-crossing procedures. It also contributes to a firm's reputation as a "secure partner" (Huang, Zhang et al. 2005), specifically for actors with trans-border operations, such as logistics service providers (Peleg-Gillai, Bhat et al. 2006). Political security initiatives, however, have a singular goal

[14] Whipple et al. found that firms agreed to a limited extent that security is a competitive advantage Whipple, J. M., M. D. Voss and D. J. Closs (2009). "Supply chain security practices in the food industry: Do firms operating globally and domestically differ?" Ibid. **39**(7): 574 - 594.

of countering and mitigating the risk of terrorist attacks and smuggling involving shipping containers, vessels, and imported goods. As such, strict adherence to regulatory security schemes will not protect a supply chain against other types of risk. It is therefore appropriate to consider many kinds of risks that threaten supply chains.

A third strategy is a reorganization of logistics operations of warehousing, production, and transport processes (Macpherson and McConnell 2007, Vance 2008). Some strategic logistics options include relocation of warehousing and production facilities to reduce dependencies on overseas sourcing (Macpherson and McConnell 2007, Vance 2008). Having plans for alterative production and sourcing sites, including formally negotiated alternative suppliers, and substitutable transportation solutions were suggested as ways to create business continuity in the face of security risks by Sheffi (Sheffi 2001) and Martha and Subbakrishna (Martha and Subbakrishna 2002). Inventory planning for security might involve inventory management strategies (Hale and Moberg 2005), including increasing inventory levels and having additional locations. Operational logistics planning for security could also potentially involve new transportation operations to compensate for problems related to cross-border delays (Macpherson and McConnell 2007) and for risks involving the transport of hazardous materials, including routing to avoid high-risk areas or mode/carrier choice. Mode and carrier choice under conditions of security risk is discussed by Meixell and Norbis (2008), where preparedness and security are additional criteria for carrier selection (Voss, Closs et al. 2009). A report from the INTEGRITY and SMART-CM project (2008) indicates that, while vulnerabilities of supply chains are recognized, there is an unwillingness or inability to increase inventory or change logistics processes. Rather, efficiencies are sought in the framework of existing processes through improved visibility, which can result in less inventory overall and more efficient transport operations (Closs and McGarral 2004, A. T. Kearney 2005).

Visibility along the supply chain can be enhanced notably by technologies including RFID attached to electronic seals and smart containers and in track and trace applications that involve GPS for permanent position tracking of containers, of vehicles, or products. Improved visibility, through application of RFID, has led to efficiency improvements, heightened security, and improved response. Process improvements appear due to more

accurate and timely shipping information and fewer delays and the resulting predictability (Peleg-Gillai, Bhat et al. 2006). Ustundag and Tanyas demonstrated supply chain performance benefits from implementing RFID system for high value products (Ustundag and Tanyas 2009). Security improvements are created when containers can be located and rerouted when necessary (A. T. Kearney 2005), and when the progress of a container can be tracked from its source (Lee and Whang 2003). Capabilities for detecting deviations from transport, delivery and inventory plans are supported by Track and Trace technologies. Müller, for example, outlines a security event management system relying on sensor-equipped smart containers, RFID and GPS that reports unexpected events involving a transport container. [15] Such events might include disruption of the container when the door is opened unexpectedly or due to tampering, or when the container comes to a standstill, specifically in an unsecure area (Müller 2008). Response to potential problems and security incidents and disasters can be improved with real-time information regarding the whereabouts of goods, the actors involved, the general process as well as certainty around the status of shipments of relief supplies from their origin to point of use in response efforts (Baldini, Oliveri et al. 2012).

A fourth strategy to mitigate disruptions in the supply chain is to build up flexibility and resilience. The requirements for flexibility for supply chain security were demonstrated by the interest in the topic by scholars and practitioners. Flexibility has been the victim of SCM principles in the past, as many supply chains traded flexibility for efficiency gains by lowering sizes of inventory buffers, narrowing the supplier base, and in general applying principles of lean management. Flexibility is, however, a means by which a supply chain can mitigate the effects of disruptions, and maintain its service to end-consumers. Adaptation was identified as a theme in the literature on SCS by Autry and Bobbit, with the topical solution of having pre-determined alternative avenues to perform business processes of distribution, sourcing, to accessing assets (Autry and Bobbitt 2008). Resilience on the other hand is the ability of a system to recover after a

[15] "The major benefits of RFID in supply chain management are also presented in Jungbae Roh et al. (2009). Theft reduction is considered the main expected benefit as it translates to cost savings in the commercial domain..." Baldini, G., F. Oliveri, M. Braun, H. Seuschek and E. Hess (2012). "Securing disaster supply chains with cryptography enhanced RFID." Disaster Prevention and Management **21**(1): 51-70.

damaging occurrence (Timmerman 1981, Peck 2005). Specifically for supply chain, resilience can be considered as the ability of the supply chain to return to normal standards of operations following a failure in one or more of its components (Willis and Oritz 2004).

To improve response and recovery from a security incident, planning is advocated throughout the literature discussing this subject as is managerial training, including on knowledge-sharing regarding available resources (Hale and Moberg 2005). Nevrous (2010) advocates building on knowledge of the potential risk scenarios that a firm could face by making investments into response capabilities. Technological means of detecting anomalies are also advocated as a means of improving response to a security breach (Autry and Bobbitt 2008). Real-time information relaying and visibility of goods and actors across the supply chain are therefore requirements to reduce vulnerability.

In response, investments need to be made into the adaptability and resilience of the supply chains (Willis & Oritz, 2004). Business continuity is therefore, and unsurprisingly, a continuous theme in research of supply chain security (Autry & Bobbitt, 2008, p. 57). Business continuity management (BCM) is defined as:

> "...the development of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise" (Hiles and Barnes 2001).

Business continuity management includes crisis management (overall processes to manage the incident), disaster recovery (recovery of critical systems, applications, data and networks), business recovery (recovery of critical business processes) and contingency planning (recovery from impact external to the organization)" (Norrman & Jansson, 2004, p. 439). The five-stage process to disaster contingency planning is: planning, detection, mitigation, response and recovery. Mitigation strategies must be: a) social, rather than physical; b) pro-active rather than reactive; c) focused on internal structures, rather than external forces; d) integrated with on-going processes; e) monitored, reviewed and modified for their effectiveness (Weichselgartner, 2001). In an analysis by Barnes and Oloruntoba (2005) the authors demonstrate how crisis management might be used to help

firms predict and detect crises and minimize losses from a damaging event. Helferich and Cook use the framework of disaster logistics to deal with disruptions in the supply chain caused by natural disasters, theft, terrorism, accidents, or similar hazards specifically calling for the 5-stage process outlined above.

While the timeliness of response is an important issue, the efficiency of responding to crisis is another. Whiting and Ayala-Ostrom found that disaster relief efforts are between 20 per cent and 25 per cent costlier than normal day-to-day operations (Whiting and Ayala-Ostrom 2009). The authors state that: "Even a small reduction in logistics costs, or narrowing of this gap between emergency operations and normative state would yield large savings", and promote performance measurement as a key way to evaluate effectiveness of logistics operations in response to disaster (Whiting and Ayala-Ostrom 2009). Disaster response, however, is complicated by degraded or destroyed infrastructure and a high degree of chaos (Baldini, Oliveri et al. 2012). This illustrates a strong requirement for high quality, efficient decision making regarding response to security events.

Finally, creating and enforcing a "security culture" has emerged as a strategy in dealing with supply chain security risks. A further consensus seems to have developed that security performance will differ between firms who will take a leadership position in security capabilities and firms who are followers, separating secure supply chain from highly secure supply chains (Peleg-Gillai, Bhat et al. 2006, Hameri and Hintsa 2009, Voss, Whipple et al. 2009). One of the differentiating factors is posited to be the supply chain security culture fostered in a company (Voss, Whipple et al. 2009, Williams, Ponder et al. 2009). That managerial support is a prerequisite for the success of security measures has already been mentioned as a finding in this paper. Security culture is a facilitator or managerial directing in creating "SCS as a priority among employees through embracing and projecting norms and values that support security-related activities and allow employees to be vigilant in undertaking SCS-related efforts" (Williams, Ponder et al. 2009). For one thing, employees trained in security can better understand the normal state of business operations and can more readily identify anomalies (Williams, Lueg et al. 2008). For another thing, security-mindedness can better prepare employees for

responding to disaster. To improve response and recovery from a security incident, planning is advocated through throughout the literature discussing this subject as is managerial training, including on knowledge-sharing regarding available resources (Hale and Moberg 2005). Nevrous (Nevrous 2010) advocates building on knowledge of the potential risk scenarios that a firm could face by making investments to response capabilities.

Supply chain security culture also extends to SC-level partnerships and investments into security-risk reducing technology for tracking, reporting and anomaly detection (Autry and Bobbitt 2008). But managerial support is not enough; security requires the participation of all members of the organizations along the supply chain. Williams, Ponder and Autry posited that a difference in organizational security culture between partners in the supply chain could impact the trust and commitment of these organizational relationships (Williams, Ponder et al. 2009). Whipple et al. found that, regarding service providers, there is room for improvement in how firms collaborate in emphasizing their partner's security capabilities. The research also found that service providers' security capabilities are more important to firms operating internationally (Whipple, Voss et al. 2009). A question arising out this discussion is: which security capabilities are required of logistics service providers, and how can LSPs fulfil the security requirements of the supply chain?

3.5 Conclusion

Security is a top driver of change in supply chain management (Hameri and Hintsa 2009). For modern supply chains, there is no longer a question of whether or not to invest in security, but how much, where, which security initiatives to comply with, who to partner with, and how to get the best return on investment. The continuity and efficiency of the value creation processes along a supply chain in matching supply to demand are threatened by security risks, which include not only the loss of assets but also the risk of malicious, man-made disaster. Moreover, the risk of losses to brand value, corporate image and reputation through involvement with a terrorist attack are significant, especially for corporations relying on strong customer relationships. Adherence to regulatory

security initiatives and the implementation of security measure along the supply chain, also present risks, as these threaten the efficiency of supply chain processes by raising costs. Therefore, security measures need to be implemented that respond to these risks by improving the security of supply chain, that make the supply chain processes more efficient, and that create resilience in the face of security disaster risk.

Towards these objectives several categories of security measures can be found. The first is the implementation of tools that create a higher level of visibility and information-sharing within a supply chain that improve communication. The second is adherence to international regulatory security initiatives. A third strategy involves changes in logistics operations or having alternatives to implementation in the case of a security incident. Another category of measures involve building up competencies in resilience and response to deal with security incidents. Lastly, creating a security culture is a strategy that could define the communication and success of the implementation of security measures.

The applications of SCM theory for increasing security in the supply chain while delivering gains in efficiency are limited so far (Thomas 2008). One of the reasons why this seems to be true is the focus within the studies of SCM on the strategic level of supply chain management, while downgrading the logistics functions on the operational level due to their being outsourced (Peck 2006). Yet, security regulations impact the physical movement of goods most directly, and therefore it is the logistics service providers and transport operators who are operationally responsible for the security of the goods. It can be concluded, then, that security is an area where the level of integration between the supply chain and transport chain plays a significant role.

Hardening the supply chain and making it less vulnerable to risks also requires a look at the design and operations of its underlying logistics operations. While transport processes are executed within the context of the supply chain, the strategy of the supply chain dictates the logistics activities, as well as their security requirements. Operational decision making should, then, be in line with the strategy of the supply chain, especially regarding security, as these will involve trade-off decisions (Sheffi 2001). Jüttner (2005) stated regarding supply chain risks, that “organizations in the supply chain must establish processes that permit them to act consistently with the philosophy and principles”. And, as

supply chains continue to evolve towards stronger strategic partnerships and integration between logistics, decision support systems will also need to evolve to support these decisions; decision processes for supply chain integration and collaboration are fundamental. For this reason, supply chain security requires support in the area of decision making that integrates (the interests of) multiple stakeholders, including integrated logistic operators.

The next chapter looks more specifically at using transport planning to increase the security of supply chain at the level of their transport processes.

Chapter 4 Logistics Planning: Mode Choice and Intermodal Logistics towards Supply Chain Security

The last chapter demonstrated the important role of security for supply chains. It was shown that security risks highlight requirements for partnerships across the supply chain in creating insight into vulnerabilities and sources of risk and taking collaborative measures to counter these risks and prepare to deal with man-made disasters and limit the impact of security events. In considering security measures, cost-benefits are sought. While cost-benefits for the supply chain are foremost achieved where efficiencies in business processes are created - most notably through the provision of timely and accurate information - security for supply chains is still a cost-driver. Nevertheless, the security risks are significant enough to justify investment, even where efficiencies are not gained immediately, such as in the area of business continuity and disaster planning.

One category of security measures given in the literature was that of logistics planning and the reorganization of transport and inventory processes to counter transport-related security risk. The purpose of this chapter is to look at existing models of transport logistics planning and their use, and to explore their applicability to the issue of security. To this end, some major issues including the relevant dynamics in the logistics industry are first looked at, followed by a review of the literature on operational planning models. Models for mode choice problems, intermodal planning problems, and routing models are looked at, identifying the decision problems under consideration, the decision makers, the factors included in the evaluation of alternatives, and the weights and values assigned to these criteria. Then the implications of security for operational logistics planning are discussed. Finally, the question of how a security construct can be incorporated into these models is explored. Some implications for modelling mode choice in logistics planning are drawn.

4.1 Logistics Planning: Challenges

Logistics planning, that is, the planning of production, inventory and transportation of goods, is done in the context of business and consumer requirements and risks.

International supply chains face security risk and, additionally, the risk of security-related delays and other sources of inefficiencies in their border-crossing operations. Within this context of business needs on one hand and security regulations on the other, requirements for supply chain security are affecting supply chains in three major ways: a) government bodies play a larger role in the operation of supply chains through the mandating of security standards; b) collaboration between actors in the supply chain is required to ensure smooth border crossing processes, requiring advanced information and visibility; and c) the costs of complying with and investing into security initiatives are leading organizations to search for ways to gain benefits in the form of process efficiencies from their investments into security.

These impacts likewise have security implications specific to logistics service providers. For one thing, there is a lot of pressure to comply with security initiatives and maintain a reputation of being a secure operator, despite the cost of doing so. This is especially true for logistics service providers who are responsible for moving goods across borders and through customs bodies. Second, because of the significance of their functions to the efficient operation of supply chains, LSPs are positioned to be integrated further into the activities of supply chains. Third, maintaining a reputation as a secure operator is central to the service offerings of LSPs.

There are constantly new challenges arising in transport management, and heightened interest in security in both the public and private sectors is only one aspect and part of a much bigger set of dynamics the logistics sector is facing. Changing customer demands call for value-added services from LSPs in value creation (Macharis, Van Raemdonck et al. 2012), especially related to information (Caris, Janssens et al. 2009), while market and competitive forces present significant challenges for logistics managers (Caris, Janssens et al. 2009). Recent historical developments in the logistics industry have also created some challenges. Shortcomings in capacity is one; limited capacity of the railways, for example, is in part due to the privatisation of rail transport operators in the EU that has resulted in divesture in transport infrastructure in the region (Meixell and Norbis 2008).

Figure 4.1 highlights some of the dynamic factors influencing transport planning coming out of dynamics in supply chain management and the logistics industry.

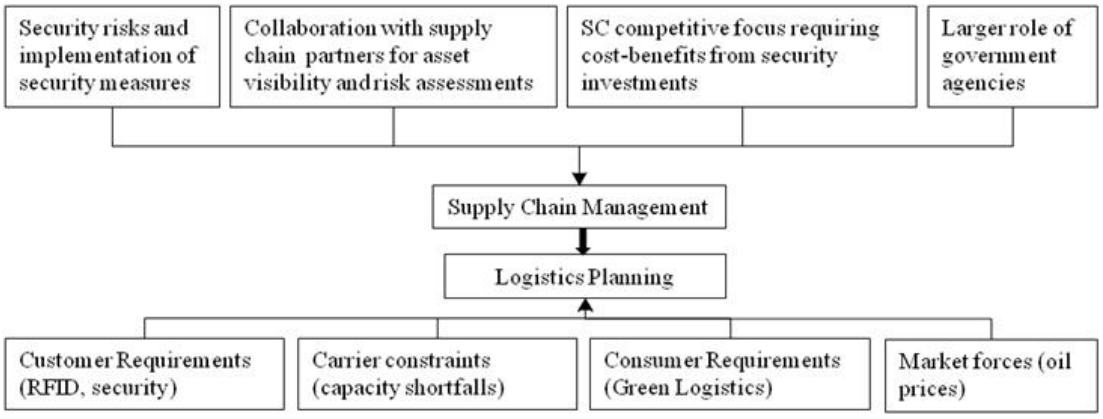

Figure 4.1 Logistics Planning in the Context of Supply Chain Security, Transport Networks (source, by the author)

Transportation networks themselves play a significant role in transport planning, and further, in achieving any operational efficiencies (Tavasszy, Ruijgrok et al. 2003). Transport networks, including transport infrastructure and operators provide both opportunities and constraints for transport planning. At the transportation network level, a significant and current development is the changing role of ports, both sea ports and inland terminals, due to their heightened functional specialization and regionalization (Notteboom and Rodrigue 2005). Likewise, there is an increased role of terminal operations in supply chains, referred to as "supply chain terminalisation" (European Commission 2009). Port regionalization infers an integration of the port operations with its hinterland logistics networks (Tavasszy, Ruijgrok et al. 2003). Accordingly, inland terminals play an important role in coordinating activities between the port and inland carriers by shifting collection and distribution activities away from the sea ports, which relaxes some of the capacity constraints existing there, and at the same time facilitates coordination with hinterland activities. This is especially important considering the impact of post-panamax container ships (Woxenius 1999) and the strain these put on the capacities at the ports and on the connecting infrastructure.

Terminals also play the role of an inventory buffer, due to the increasingly common conceptualization of "inventory in transit" and "inventory at terminal" (European Commission 2009), whereby goods underway are considered to be inventory en route. The push for more visibility in the supply chain has meant that goods in transit are "visible" to supply chain partners, and can therefore be integrated into inventory systems' calculations.[16] Terminals at sea ports or inland consolidation centres are therefore temporary inventory buffers. This means that port operators have a greater decision making role as ports and inland terminals are imposing time limitations and time charges on their customers for service operations.

Another major hurdle to overcome in transport planning is the coordination of the decision making tasks between multiple decision makers. Logistics activities involve a high number of interacting actors that include both public and private interests and cover industrial players involved in all areas of manufacturing and distribution. Decision support in the area of logistics, then, has to be able to deal with multiple stakeholders and objectives, which is a knowledge area explored explicitly by operations research and management science (OR/MS). OR/MS methods are able to take into account multiple decision makers and the resulting goal conflicts.

Despite the relevance of multiple decision makers in logistics problems, however, there is relatively little research in the literature that deals with multiple stakeholders (Macharis and Bontekoning 2004, Macharis, Pekin et al. 2008). One area that is specifically affected by the presence of multiple stakeholders on the supply chain is that of sharing the value that is created by the activities of a supply chain. *Value* in this context can be considered to be the difference between the customer value (revenue) and the effort expended in creating this value, where this value is then augmented by either reducing the overall supply chain costs or by increasing the revenue (ISO 2007). Lowering the overall costs can be achieved through supply chain integration, specifically in the logistics context; however, value sharing across supply chain actors - not only the shippers, who are most

[16] This is also referred to as "mobilized inventory", and is blurring the line between the fixed cost calculations associated with stationary inventory and variable costs associated with costs of transportation Hesse, M. and J.-P. Rodrigue (2004). "The transport geography of logistics and freight distribution." Journal of Transport Geography **12**(3): 171-184..

likely to benefit - is important in creating stable, integrated collaborative relationships (ISO 2007, Stadtler 2008).

Real-time decision making is another aspect of growing importance for transport planning. Technological changes in communication and transportation systems, namely the availability of real-time, event-driven data and automation of logistics operations, pose approaches to support real-time, event-driven decision making and, further, optimization of automated systems. Along with the technical aspects that allow real-time data to be captured, there must be organizational rules that make real-time decision making possible in order to capture the benefits of rapidly-available information in decision making. For example, operational decision making in real time occurs in planning for truckload carriers (Crainic, Kim et al. 2007), as these frequently have to deal with unplanned delays and consequential late arrivals, unplanned demands or cancelled requests, which result in additional empty runs. Models for fleet planning can handle real-time information to minimize the number of empty container movements, if the information is received in a timely manner (Crainic, Kim et al. 2007).

Planning models *for the level of the system and service network design*, however, are required to capture and use the information from automation equipment at terminals for optimization of automated terminal operations (Crainic, Kim et al. 2007). More often, planning models at the tactical and strategic levels are not able to make use of real-time information, as these are static and deterministic, and thereby do not capture the stochasticity of real-life uncertainties.

Traditional hierarchical organizational structures separate decision making functions from the information and knowledge that is required to make good decisions (Sanchez and Heene 2004). Not only does the quality of the decision suffer, but the rapidity with which decisions can be made and action is taken is significantly impeded. A managerial shift to empower functional teams with decision making authority overcomes this difficulty. In this case, the role of top management is to provide the structure in which the decisions are to be made. Decision policies are then set, so that action is taken within the boundaries of

a previously set strategic direction. This organizational form of devolutionary decision making is illustrated by Figure 4.2.

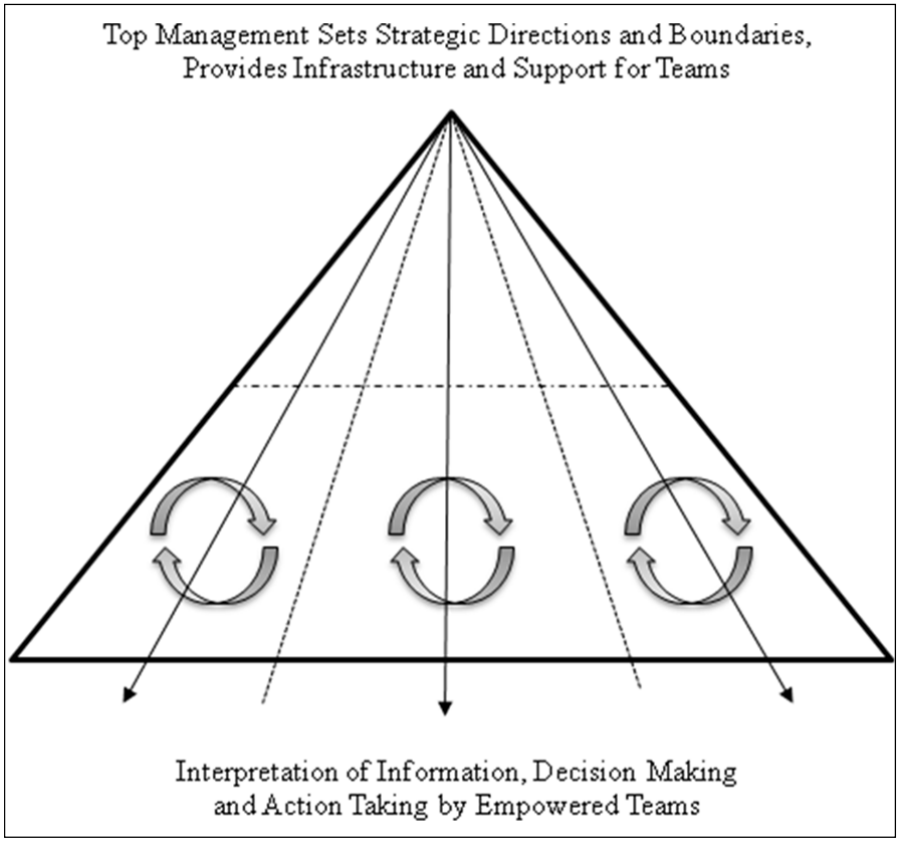

Figure 4.2 "New Forms" of Flat, Team-Based, Empowered Organizations (Sanchez and Heene 2004)

Supply chains can benefit greatly by such devolution of decision making authority to functional teams. Theoretically there are no limitations that the structure of these teams cannot cross functional borders, managerial levels, or company borders. Supply chains, both cross-functional and trans-organizational, stand to benefit from new managerial forms and strategic policies that would allow for real-time decision making.

Regarding security in logistics, it is important that decision structures allow for real-time, event-driven data, allowing for fastest response times to any event that could compromise a container or movement of goods. In this way, the data captured and related from an information system can be acted upon in a timely fashion. Real-time rerouting of

transports, for example, in the case of dangerous or HAZMAT goods, would provide security benefits, in the case of risk profiling.

Until now, little research has been done towards real-time decision making, especially in regards to the security of supply chains and logistics processes.[17] Research is being done in the area of online decision making to dynamically solve decision problems in order to deal with uncertainty and unplanned events as they occur. The two main methodological means of dealing with uncertainty dynamically are having fixed revision times for decisions that take into account new information, or event-triggered revision of decision making. In the latter methodology, it is possible to automate dynamic problem solving, if defined rules are adhered to (Schönberger and Kopfer 2009).

4.2 Logistics Planning: Transport Mode Choice

The mode choice problem is a fundamental one to freight transportation decision making. For one thing, the choice of mode is a great cost factor in total logistics costs (TLC) affecting not only transport costs, but also inventory carrying costs, purchase cost, and order cost (McGinnis 1989, Dullaert, Vernimmen et al. 2007). For another thing, mode choice relates to the overall logistics strategy of an organization; production and inventory policies as well as upstream and downstream relationships play a strong role in determining mode choice. Finally, aggregated mode choice behaviour, or *modal split*, represents a key input for public transport policy, which, in turn, establishes long-term parameters for decision-making in mode choice (Banister and Berechman 2000, Crainic, Kim et al. 2007). Highlighting the importance of modal split, it has become the focus of public policy in the EU, where there is a concerted effort to move away from road transport and to encourage more efficient freight transport as part of its "sustainable mobility" concept towards environmental protection (EC 2008). The mode choice problem, then, is a central one to logistics planning and one that impacts total logistics costs for supply chains, is constrained by supply chain strategy, and is impacted by (and impacts) public policy.

[17] This is the subject of the EU FP7 Cooperation Work Programme Security

4.2.1 Mode Choice as a Determinant of Total Logistics Costs

Investigation into transport mode choice has moved from a historical assumption of minimizing total costs between two or more modes of transport and increasingly incorporates a significant number of service-oriented factors. Historically, the transportation mode choice decision was modelled using a cost-minimization function (McGinnis 1989), which compared the direct transportation costs of two or more transport modes over a range of distances. Later, indirect costs in the form of inventory carrying costs were included. Inventory costs result from the reliability of arrival times, transportation time, and expected losses underway. Total logistics cost calculations handled these cost-service trade-offs. Models to calculate TLC were put forward by Sheffi (1985).

Total logistics costs, consisting of the costs for transportation, inventory and warehousing, administration, and order processing, is an important indicator of supply chain efficiency (Vernimmen, Dullaert et al. 2008). TLC relates supply chain costs to the choice of mode transport due to the impacts of the modal choice on order costs, inventory costs, and purchase costs, so that TLC is comprised of order cost, transport costs, costs of cycle stock, costs of inventory in-transit, and costs of safety stock (Ballou 1999, Vernimmen, Dullaert et al. 2008). The total cost approach, therefore, reflects an integrated view of manufacturing and inventory scheduling that evolved in the 1990's to lower to effects of the Bullwhip effect across the supply chain (Stonebraker and Afifi 2004). From the TLC perspective, it is easy to conclude that shorter transportation times result in lower in-transit stock and safety stock and associated costs. The trade-off for these lower inventory costs is the resulting higher transportation costs, but transportation modes that allow for shorter lead times and order cycles result in lower total logistics costs overall. The time compression and flexibility offered by road transport, therefore, makes this mode more attractive than both rail and barge transport, despite higher direct transport costs (Vernimmen, Dullaert et al. 2008).

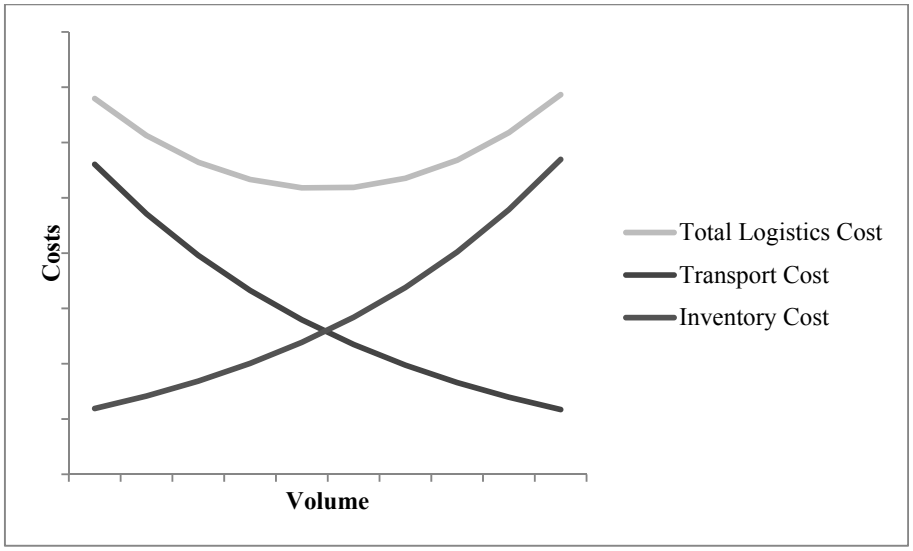

Figure 4.3 Total Logistics Costs – Trade-offs in Transportation and Inventory Costs

The inventory-theoretic model takes the mode-dependent changes in inventory costs into account, and is able to quantify the trade-off between transport costs and inventory costs as they relate to the different transport modes. It is found that the higher transport costs for transport by truck are offset by lower inventory costs in safety stock, due to shorter and more flexible lead time. In the same manner, the lower per tonne transport costs for the mass transport modes inland navigation or rail transport, which decrease with an increase in the volume transported, tend to be negated by higher inventory costs resulting from the higher costs of cycle, in-transit, and safety stocks. Slower and less reliable lead times and larger loading capacity that characterise transportation by inland navigation and rail service are the causes for the higher levels of inventory that are required when these freight transportation modes are selected (Dullaert, Vernimmen et al. 2007, Vernimmen, Dullaert et al. 2008).[18] The inventory theoretic models that capture the quantitative effects of mode choice on inventory and order costs on total logistics costs, however, do not capture non-quantifiable aspects of transportation mode choice, such as

[18] Consolidation, and system and service scheduling on shorter lead times would mean that the difference in costs between relatively large and small loads would not differ too greatly, while higher frequency and more regular shipments would lower the order quantity. One important development for intermodal logistics is that terminals (sea ports and inland terminals) are used as storage buffers and consolidation centres European Commission (2009). A sustainable future for transport. Towards an integrated, technology-led and user-friendly system..

behavioural differences among shippers or characteristics in shipper markets (McGinnis 1989).

4.2.2 Strategy as a Determinant of Mode Choice

Transport and logistics considerations have been increasingly integrated in production and inventory systems, and a total transport cost concept evolved (Stonebraker and Afifi 2004), bringing not only transport costs and inventory costs into the calculation, but also qualitative factors, the foremost of which is reliability of delivery times (McGinnis 1989).[19] Accordingly, production systems and characteristics of the goods themselves have become determinants in the selection of the mode. In the extreme case, transport and logistics issues have been taken into account during the product design stage as part of the supply chain design process.

The shift to incorporate logistics processes into the design of production systems has meant that the consignments have gotten smaller with higher frequency; the opportunities for consolidation are less, at least where a single shipper is concerned and where possibilities for consolidation between shippers are limited. A survey done by the Institüt für Mobilitätsforschung in 2007 showed that shippers who employed a Just-in-Time inventory approach or a Just-in-Sequence production scheduling approach require a high degree of reliability in delivery times and arrival time of undamaged goods (Institut für Mobilitätsforschung 2007). These systems naturally gravitate towards road transport. In highly dynamic environments, characterized by a large product range, more complicated products with shorter product life-cycles, and unpredictable demand, the costs of safety stock rise more quickly than in less dynamic environments. These developments have led to the heavy use of road transport, which offers faster, more flexible service, providing shorter lead times and the means to reduce safety stock.

The different freight modes offer different levels of capabilities that answer to transport demand in different ways. Ihde (2001) recommends a structure for the advantages offered by the different modes by evaluating them along varying degrees of:

[19] It was postulated that flexibility in the logistics and transport will be of less importance in the future, as production systems become more flexible.

1. Capacity: ability to carry large masses of goods at low costs
2. Speed: transportation time, lead time
3. Spatial coverage: ability to traverse spatial areas
4. Reliability: ensuring the timeliness of delivery and the condition of the product
5. Flexibility in time: ability to adapt to different market/demand cycles, including changes in the sizes or frequency of the shipments
6. Spatial flexibility: transferability between means of transport and capacity sharing
7. Safety and security: low accident and damage rates

Road transport offers the greatest degree of spatial coverage, speed, and flexibility. As a consequence, road transport has seen the greatest gains in volume, and has won market share over rail and waterway transport.

The selection of freight transport mode, while not necessarily done directly by the shipper, is therefore based on how the impact total logistics cost and fit with the logistics strategy of the supply chain. The mode choice, then, has been shown to be determined by several factors. These factors (also referred to as attributes) and their weights of importance in determining mode choice have been studied and discussed in the literature. A cost-service trade-off based on the transport mode is the most recognized determinant of mode choice. "Service" is used rather ambiguously in this context for a combination of determining factors, but the most predicative factors of mode choice have been shown to be: cost, reliability of arrival time, low probability of damage and loss to goods, and availability (Bontekoning, Macharis et al. 2004, Institut für Mobilitätsforschung 2007). At the same time, Cullinane and Toy (2000) showed that the most researched attributes were cost, speed, reliability, characteristics of the goods, and service.

The relative importance of these selection criteria, however, is not constant, and the utility of transport mode attributes depends on characteristics of the goods, shipment sizes, the industry, as well and production and inventory systems (Danielis, Marcucci et al. 2005, Witlox and Vandaele 2005, Institut für Mobilitätsforschung 2007). Distance and shipment sizes are also determinants of the mode's utility (Vannieuwenhuyse, Gelders et al. 2003).

Many studies have been made into the relative utility of the various attributes of modal systems. McGinnis examined 11 empirical studies, finding that cost - under several various terms - was always an important factor, but was consistently less important than at least one other variable (McGinnis 1989). Another study by Vannieuwenhuyse found that cost, safety, reliability, transportation time, and flexibility were the preferred attributes in selected transport modes for shippers and LSPs (Vannieuwenhuyse, Gelders et al. 2003). These findings were reiterated by Cuillinane, who found that reliability (transit time variability), transportation time (speed), and cost to be the most influential attributes, while loss and damage (safety) and a range of other attributes were of secondary importance (Cullinane and Toy 2000). Further, the works of Danielis et al. (2005) and Witlox and Vandaele (2005) quantify the utility of mode attributes. In the first paper, the authors found heterogeneity of freight transport mode attribute utility between sectors as well as between inbound and outbound flows (Danielis, Marcucci et al. 2005). They reiterate the findings that companies employing a JIT inventory approach are more sensitive to late arrivals and changes in travel time. The paper of Witlox et al. looks at several cases of mode choice selection criteria to find monetary trade-off levels between mode attributes (Witlox and Vandaele 2005). For the attributes reliability, frequency and travel time they found a willingness to pay for increasing quality of service.

Modal characteristics are not the only factors that are taken into consideration in the mode choice decision. The characteristics of the goods, the spatial and temporal nature of the shipments, and, as mentioned previously, the supply chain management strategy determine mode choice. Moreover, less rational factors, such as the relationships between the shipper and carrier, as well as the image the shipper holds of a particular mode, past experience, and trust and relational factors that exist between the shipper and the freight forwarder (Vannieuwenhuyse, Gelders et al. 2003).

Table 4.1 gives an overview of the five main categories that have been dealt with in the literature as determinants of transport mode choice.

Table 4.1 Determinants of Mode Choice (adapted from CUTR 2000)

Determinate Category	Attributes
Total Logistics Costs	Order and Handling Costs Transportation Charges Loss and damage costs Capital carrying cost in transit Inventory carrying cost at destination Unavailability of carrying costs Service reliability costs Intangible service costs
Physical Attributes of Goods	Shipment size Package characteristics Shipment shelf life Shipment value Shipment density
Flow and Spatial Distribution	Shipment frequency Distance of shipment
Modal Characteristics	Capacity Trip time and reliability Equipment availability Customer service Handling Quality – Damage and Loss Reputation
Behavioural Attributes	Shipper's perception of the mode Shipper/carrier relationship

Mode choice, consequently, can be seen to shift with dynamic forces in the logistics industry, including evolving processes in production and supply chain management.[20]

4.2.3 Mode Choice as an Input for Public Policy

Across Europe, the current modal split, that is, the percentage of goods that are carried by transportation modes, heavily favours road transport. The current predominance of road traffic over other modes is not desirable, nor is the growth in volume of road transport

[20] The impact of dynamics discussed earlier, including shorter product life cycles, continued globalization and growth of emerging markets and increased product customization, on the development of logistic systems include a trend toward decentralization of logistics networks, supported by improved flow of information due to increased use of ICT systems Tavasszy, L. A., C. J. Ruijgrok and M. J. P. M. Thissen (2003). "Emerging Global Logistics Networks: Implications for Transport Systems and Policies." Growth & Change **34**(4): 456-472..

sustainable over the long term, having higher social costs in road safety, traffic congestion, and noise pollution and air pollution than rail and inland navigation. This pattern favouring road transport is also inefficient in its use of available infrastructure and capacities; reliance solely on road transport does not take advantage of the capacities and capabilities offered by multimodal transport. Rather, heavy use of road transport leads to higher external costs, such as accidents, noxious emissions, noise, and congestion, a large percentage of which could be avoided with stronger use of multimodal transport (Macharis, Pekin et al. 2008).

Mode split is a major issue for transport policy. The increasingly large volume of freight transport requires better solutions for the future to solve problems of increasing congestion on the roads and related safety concerns, as well as ecological and environmental externalities of water and air pollution, and noise pollution. EU policy is concerned with getting freight transports off the roads and onto the more environmentally friendly shipping lanes, inland waterways, and rail lines for the maximum portion of freight hauls (van Duin and van Ham 1998):

> Concerning freight transport, an intelligent and integrated logistics system must become a reality, where development of ports and intermodal terminals is a key element. Finally, the urbanisation trend…will make a 'modal shift' towards more environment friendly modes particularly important in the context of urban transport (European Commission 2009).

However, since transport policy in the EU has not come so far as to force an internalization of these external costs, road transport is still more cost efficient, especially over relatively shorter distances than in combination with rail transport or inland navigation. The relative shares of freight transport for the transport modes road, rail and inland waterway for the EU 27 region are presented in Figure 4.4 (Eurostat 2009).

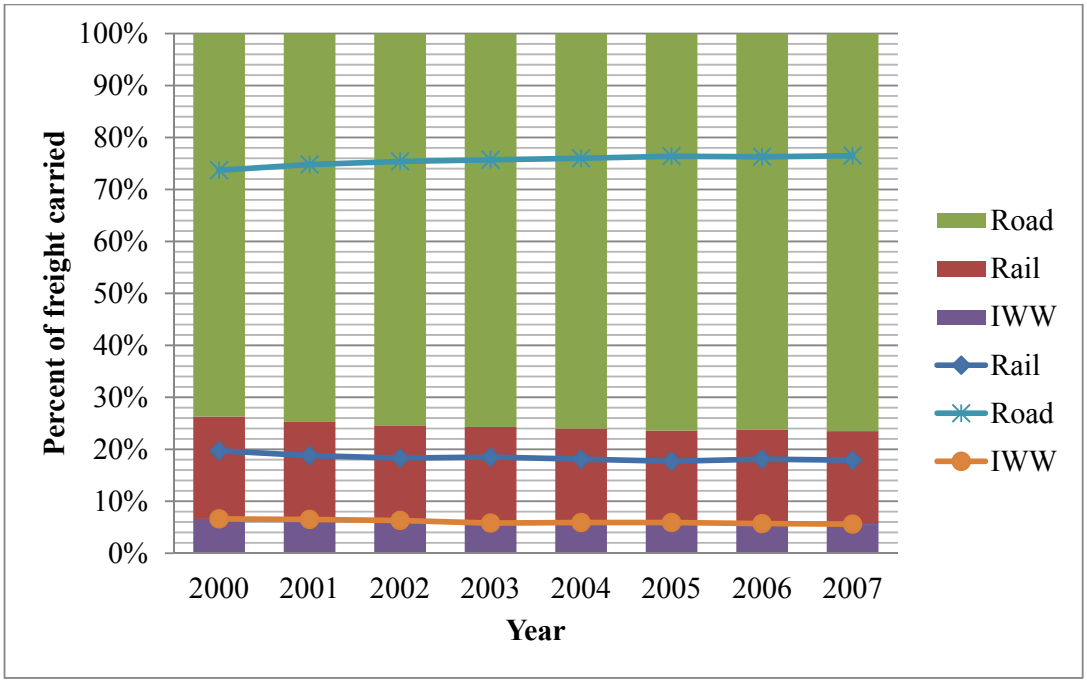

Figure 4.4 Modal Split (as %) of Road, Rail and Inland Waterway Freight for the EU 27

Options for improving the modal split from a policy perspective include, for one, forcing an "internalization" of external costs, for example by excising a toll on road traffic, which would move the break-even point in favour of intermodal transport. Another option is through subsidization of inland waterway transport or rail freight operations, to likewise make these more cost-competitive against road hauling. Another long-term strategy within the EU has been to invest heavily into rail and waterway infrastructure to increase the capacity of freight corridors, specifically for trans-border freight, for example in the Marco Polo projects. Relieving bottlenecks and increasing reliability and transport time for shipments per rail and inland barge has also been sought through investments and implementation of ICT, including traffic management systems (European Commission 2009).

4.3 Intermodal Transport Planning

Intermodal transport has been made possible due to the development of a standard loading unit (i.e. the shipping container), that can be transported by various means of

transport, as well as the standardization of container shipping, has (Macharis, Van Raemdonck et al. 2012). Intermodal transport is classically defined as "the movement of goods in one and the same loading unit or road vehicle, which uses successively two or more modes of transport without handling the goods themselves in changing modes" (ECMT 2001).[21]

The benefit of using intermodal transport is considered to be the ability to take advantage of the service offerings of the single modes to their best advantage. The transportation policy in the EU strongly supports intermodalism as a means of coping with increases in transport volume while reducing congestion, roadway accidents, and environmental concerns connected with the high volume of roadway traffic (Bontekoning, Macharis et al. 2004), including noise and air pollution, since intermodal transport offers a great opportunity for efficiency regarding capacity use over use of a single mode, especially road transport.

The difficulty in taking advantage of this potential lies in the coordination of intermodal operations due to the involvement of various operators, and the costs that arise due to transhipment that do not occur when a single mode is used, so that the cost advantages of using mass transport modes are offset by the cost of transhipment and pre- and post-hauls, performed most often via road transport. The cost function of intermodal vs. that of uni-modal road transport is pictured in Figure 4.5 below.

[21] Haasis distinguishes between *intermodal* and *combined transport* in that the latter refers to intermodal transport where rail, short sea shipping or inland shipping accounts for the greatest portion of the carriage, and where road carriage is minimized Haasis, H.-D. (2008). Produktions- und Logistikmanagement : Planung und Gestaltung von Wertschöpfungsprozessen. Wiesbaden, Gabler..

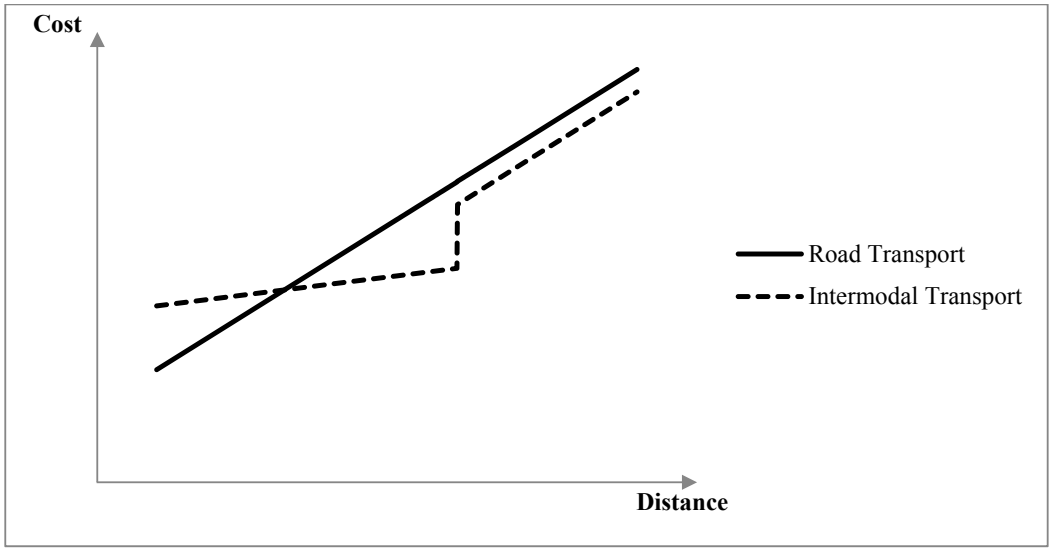

Figure 4.5 Cost Structure of Intermodel Transport vs. Road Transport (Macharis, Pekin et al. 2008)

In order for intermodal transport to be competitive against road traffic, then, it must be able to take advantage of the individual benefits provided by the different modes. The transhipment and disposition processes at terminals and rail yards need to be efficient in order to minimize average costs of container through put and time delays, which factor heavily into discouraging the use of intermodal transport over uni-modal transport. Higher transportation costs in general, however, for instance those resulting from high oil prices, may present some opportunities for alternative modes of freight transport (INTEGRITY and SMART-CM 2008, Macharis, Van Hoeck et al. 2010):

> But how do the stakeholders react in this boom in transportation costs? According to UNCTAD there is anecdotal evidence that some major shippers are considering adapting their inventory policy to reflect higher transport costs which have as base the high demand and absorb the increased transport costs. Such strategies followed by big shippers, carriers and logistics services providers are...turning from road transport to alternative modes of transport such as rail....(INTEGRITY and SMART-CM 2008)

Likewise, security may have similar impacts, first in avoiding high-risk paths, and secondly, in response to a security attack in providing alternative modes of transportation.

4.4 Modelling Intermodal Transport Planning

Recent research investigates intermodal freight transport as its own area of study (Macharis and Bontekoning 2004, Macharis, Van Raemdonck et al. 2012). Operational and planning issues for intermodal transport relate to system and service design for intermodal transportation networks, container fleet management, container terminal operations and scheduling, and national planning (van Duin and van Ham 1998, Crainic, Kim et al. 2007). While intermodal transportation is more complex to model than uni-modal transport (Macharis and Bontekoning 2004), OR/MS methods, such as linear programming, integer programming, non-linear programming, network analysis and simulation methods have been found to apply to intermodal transport problems (Bontekoning, Macharis et al. 2004, Crainic, Kim et al. 2007), for example in operational planning. Other issues persisting in the area of intermodal transport research include: stakeholder interest in and hindrances in the use of intermodal transport (van Duin and van Ham 1998); shippers' interest in intermodal transport in creating a "green image"; relief of road congestion; higher transport costs (Tavasszy, Ruijgrok et al. 2003). Besides these considerations, modelling the coordination of decision making between the various actors involved in intermodal transportation (van Duin & van Ham, 1998), opportunities for shipment consolidation and mode choice are major research areas that require application of methodologies for analysis (Bontekoning, Macharis et al. 2004). Caris (Caris 2010), Caris et al. (Caris, Janssens et al. 2009) and Macharis et al. (Macharis, Pekin et al. 2008) present a good overview of operations research applications in transportation planning problems, broken down by planning level (strategic, tactical and operational planning levels), as well as by decision maker (drayage operator, terminal operators, network operators, and intermodal operators).

The lack of research to improve collaborative decision making that was pointed out by Macharis and Bontekoning (2004) and Macharis et al. (Macharis, Van Raemdonck et al. 2012) is especially relevant in the case of intermodal transport, which inherently involves multiple actors. The limitedness of the research on intermodal transport for multiple decision makers undermines its ability to provide the decision support that is required to

assist in improving intermodal flows. The tools that are available for decisions support for multiple decision makers are outlined by Van Duin and Van Ham (1998). Table 4.2 gives an overview of the limited literature dealing with multiple decision makers in intermodal transport:

Table 4.2 Research on multiple decision makers in intermodal transport (Macharis, Van Raemdonck et al. 2012)

<table>
<tr><th rowspan="2">Decision maker</th><th colspan="6">Time horizon</th></tr>
<tr><th colspan="4">Strategic</th><th>Tactical</th><th>Operational</th></tr>
<tr><td>Drayage operator</td><td rowspan="4">Macharis 2004</td><td></td><td rowspan="4">Gambardella, Rizzoli and Funk 2002</td><td></td><td></td><td></td></tr>
<tr><td>Terminal operator</td><td rowspan="3">Van Duin and Van Hamm 1998</td><td rowspan="3">Evers and De Feijter 2004</td><td></td><td rowspan="3">Bostel and Dejax 1998</td></tr>
<tr><td>Network operator</td><td></td></tr>
<tr><td>Intermodal operator</td><td></td><td></td><td></td></tr>
</table>

4.5 Transport Planning towards Supply Chain Security

It was established in Chapter 2 that security issues, especially those relating to compliance with international security regulations and standards, including associated costs and potential efficiency gains, have risen in importance in the logistics industry. Impacts of security regulations and, consequentially, of security initiatives on supply chains include:

- Additional costs, both direct and indirect
- Direct security benefits
- Improvement in business processes through collaboration and information sharing
- Heightened reactivity and resilience

Five main strategies towards supply chain security can be identified, including:

- Improved communication and collaboration along the supply chain
- Compliance with security regulations
- Logistics planning and improvements in warehousing and inventory, production, and transport processes
- Building of capabilities in flexibility and resilience
- Creation of an organizational security culture

In this context, security is considered to be "the set of activities (and physical improvements) aimed at preventing, detecting and recovering from disturbances and intrusions in the physical flow of materials between and origin and a destination over a combination of means of transportation". [22] Drivers toward these activities include:

- Heightened awareness of security risk

---

[22] See Section 3.2 for a listing of definitions in the literature of supply chain security.

- Security regulations
- Pressure from supply chain partners towards compliance and certification

It was further discussed that, while all actors are affected by security risks and regulations, the costs of implementation and the value-benefits resulting from supply chain security initiatives are not equally shared. Specifically, investments into physical access/security represent the greatest expenditures (Hameri and Hintsa 2009), and related costs are therefore borne most directly by operators with significant storage areas: warehousing operations, sea ports, inland terminals and railway terminals.

The Transportation Research Board points out that transportation systems are vulnerable to security risks due to the accessibility, extensiveness, lack of redundancy, diversity of ownership and operating, and internationality that characterize them (Transportation Research Board 2002). Therefore, one study on securing transport infrastructure proposed the following key areas for analysis (DNV Consulting 2005):

1. Vulnerability to attack, described as the possibility of an attack being successful;
2. Consequences of an attack, including the potential for loss of life, destruction of critical infrastructure and disruption (and criticality) of transport flow.

At the operational level, the characteristics of transport systems can be examined for the vulnerabilities. While considering the qualities of the transport modes themselves cannot provide a complete analysis, the different modes can be compared on how vulnerable these are in comparison to one another: Security indicators for the different modes were proposed in one study done by the ISL (2006) as a basis of comparison:

1. accidents
2. damage
3. loss of cargo
4. fire
5. dangerous cargo
6. terrorism
7. theft

The first four indicators represent an aggregated potential for loss of goods, which can be considered as a service attribute of the mode. The fifth and sixth indicators, carriage of dangerous cargo and terrorism, respectively, represent that risk of the transport to be used as a "Trojan horse" (see Section 2.1), where a malicious group takes advantage of transportation networks, facilities or assets for malicious purposes.

Regarding theft, one aspect of transport systems having particular impact on the security of freight transport is the necessity of waiting times and the length of waiting times where the freight is at rest. Freight is considered to be more vulnerable at rest than when it is moving, i.e., freight at rest is freight at risk. At the same time, freight stored in terminals and facilities with security measures in place is less vulnerable than freight stored in open and unsecured areas. So, freight needs to be stored in areas where physical access to the goods is limited to authorized personnel, even when the freight is shipped in sealed and locked containers. One report estimated that of all incidents of logistic theft, 15% of the time the goods were in a logistics facility, while for another 61% of the incidents the goods were in transit (Weise 2005). The transport modes road, rail and inland waterway can be compared, then, for vulnerability of the goods during transport time, based on in-transit delays and unsecured (though short-term) storage. In the EU, both road and rail transport are subject to legal requirements for safety of drivers and other users of transport infrastructure that lead to such in-transit delays; for example, for road transport, restrictions are placed on the numbers of driving hours of an operator. The vulnerability of freight (e.g., a container) at rest would, in contrast, decrease in the presence of technical security measures, for example, a GPS tracking system of a shipment with real-time alarm for status changes in the container (e.g., container door opening) or access security measures at warehouse, production facilities or port areas, such as those outlined in the TAPA guidelines and the ISPS code.

Other key factors in the mode choice decision, specifically flexibility, cost, speed, and reliability, are impacted by security requirements, initiatives and regulations. Mode choice therefore represents an opportunity for supply chain actors, even those not acting at the

transportation network level, to improve the security levels of their freight transports through logistics planning.

4.6 Chapter Summary

Just as supply chain management is evolving, so are the logistics systems and transportation networks that support them. Transport networks, including railway systems, inland navigation, and road transport as well as intermodal networks are complex, and distinguish themselves with emergent properties, which "arise at a particular level of system description by virtue of the interaction of relatively simple lower-level components (Caris, Janssens et al. 2009). Therefore, transport systems can be evaluated on their performance for creating and supporting efficiencies in logistics transactions, and as a consequence of the performance quality of transport systems, transport mode selection is an important consideration in transport planning.

The major issues in the mode choice problem concern its contribution to total logistics costs while fulfilling quality requirements of supply chain value creation activities, as well as using transport selection can improve performance of supply chain initiatives through integration of the transportation function.[23] Factors considered in planning for transport and routing are both qualitative and qualitative, and that specifically qualitative factors have grown in importance as logistics and transport have become increasingly incorporated in the design of production and inventory systems. Transport mode choice is also a potential area for operational decision making to promote supply chain security; specifically, the characteristics of the transport modes and their relation to vulnerabilities to security risks can be considered in the mode choice decision in logistics planning. These factors include, then, cost, flexibility (as a function of time required for advanced booking, transport time, loading, unloading and groupage of shipments), reliability (of delivery times), and risks for both loss and damages and security risks.

Modelling the mode choice problem, then, must take into account these factors, for which operations research methods, including multi-objective programming, are suitable.

[23] The literature on this point, however, is sparse (Meixell and Norbis 2008).

The next chapter will build a model to incorporates the mode characteristics to make trade-offs among transport goals for flexibility, reliability (of arrival time), transport costs, and security.

Chapter 5 Model Building for Mode Choice

The previous chapter discussed the characteristics of the mode choice problem and the factors that were shown to be considered in mode choice planning. The complexities of intermodal planning were outlined, followed by a discussion of factors that were relevant for supply chain security in transport planning. Further, it was stated that multi-objective approaches are suitable for decision making applications regarding mode choice, as these approaches model the trade-offs between competing objectives in the decision making context.

This chapter puts forward a goal programming model as a multiple-criteria decision making tool for the transport mode choice problem specifically related to the impact of security measures on the mode choice decision.

Some assumptions made in model concerning supply chain security include:

- The characteristics of the transport modes in terms of speed, flexibility in the scheduling of shipments, potential for loss through theft and damage, security risks, reliability of travel and arrival time, and transport costs shift with the introduction of encompassing security measures on the level of the infrastructure, the operators, and physical assets
- The impacts of security measures in terms of rates of loss through damage and theft, security risk, flexibility, reliability and costs are due to increased requirements for scanning/screening, investments in technology and personnel, especially training, and physical facility/asset security measures. Costs and impacts of compliance with security codes such as Authorized Economic Operator (AEO) are taken into account, as compliance requires fees for processing of applications, as well as additional processing of documentation.

Three scenarios are developed for comparison using the model in order to identify the impact of security issues on mode choice. The scenarios that are developed for analysis include:

1. Prior to regulations (base scenario with no security measures)
2. Post regulations without compliant AEO status
3. Post regulations with compliant AEO status

The transport modes under consideration are road, rail and inland waterway, and include combinations of these modes.

Two hypotheses are made on how security regulations and requirements impact mode choice. Some propositions concerning the impact of security regulations on the determinants of mode choice are put forward. Next, a hypothetical decision environment is described, within which three scenarios are developed to look at the issues typically involved in a transportation decision problem.

Concluding this section is a discussion of the results of the model and implications for further research.

5.1 Contribution of Management Science to Decision Making

The role of management is one of decision making; and a manager's task is to sort through the complexity of their environment and the dynamics relating to a decision problem. Decision support models have the role of facilitating a deeper understanding of environmental complexity (Drucker 1973). Towards understanding the decision making process, models expose underlying assumptions and missing information about the decision environment (Little 1970).

Management science and operations research encompass a large repository of modelling approaches, techniques and methodologies to support rational decision making. However, such modelling techniques are not used by managers, or decision makers, and for some very good reasons: the models are complex to build; they are difficult to understand by someone not trained in OR methods, including managers, who are ideally the users of them. The difficulty in communicability of the methodologies and methods used by OR models limits their application to experts only (van Duin and van Ham

1998)[24]. Not only are the methods self-limiting in their complexity, but the methods that come out of OR/MS lack applicability (Altay and Green 2006). A related problem is that of modeller's bias, whereby the output is pre-determined to reflect the modeller's desired solution. Another difficulty is the requirement for data and information that is often time-consuming and difficult to acquire. The models are, then, often incomplete regarding pertinent factors for decision making, often qualitative and subjective factors that are not easily quantifiable (Little 1970). However, technological changes in communication and transportation systems, namely the availability of real-time, event-driven data and automation of logistics operations, pose approaches to support real-time event-driven decision making an optimization of automated systems by improving access to more information about business processes.

Despite their limitations, the modelling techniques put forward by operations research supply principles and approaches for modelling, which, applied even partially, can readily support information gathering, analysis and understanding of complex issues.

5.2 Modelling Transportation Mode Choice

Mode choice models describe how products or groups of products are assigned to transport modes (Crainic, Kim et al. 2007). Due to the number of determinants in the mode choice problem, it was put forward that constrained optimization models deal best with the range of variables and conflicting attributes that have been shown to be taken into account by shippers in mode selection (McGinnis 1989, Meixell and Norbis 2008). The mode choice problem with the many factors that are involved, the constraints and the multiple decision makers is a constrained optimization problem (McGinnis 1989). Operations research and multi-criteria decision making (MCDM) offer methods for dealing with these kinds of problems (Vannieuwenhuyse, Gelders et al. 2003, Bontekoning, Macharis et al. 2004, Caramia and Guerriero 2009).

Challenging dynamics in the logistics industry have complicated the development of decision models due to the difficulty of quantifying them, such environmental effects and

[24] Citing: Mulvey, John M, 'Part 3. Models in the public Sector; Success, Failure and Ethical Behavior' in 'Ethics in modeling', pp. 58-73, PERGAMON, ISBN 0 08 0419305, 1994

security. Meixell and Norbis, in a recent review of mode and carrier selection literature, found that there is very little research dedicated to security issues, and specifically point out that it is difficult to quantify criteria and weights in evaluating these attributes (Meixell and Norbis 2008).

Of the literature they found, OR methods are used to identify alternative routes, provide a means of differentiating these routes (route heterogeneity), and support selection of a route from among the alternatives based on the preferences of a decision maker (Prato 2009). Prato found k-shortest path algorithms, simulations, and constrained programming as applied methods represented in the literature on mode choice. Applications of OR for route planning where security is taken into account notably include research into HAZMAT routing, for example by Erkut and Ingolfsson (2000) and Sherali et al. (Sherali, Brizendine et al. 1997). The models developed in both of these papers consider routing HAZMAT transports away from areas with higher risk of accidents or higher consequences of an accident involving HAZMAT transportation, such as highly populated areas. These models deal expressly with low-probability high-consequence risks. A review of this area of literature is given by Luedtke and White (2002). The literature on HAZMAT transport criteria and risk analysis systems is also reviewed by Macharis et al., who compare risk evaluation methods, and propose a refined MCA approach involving that accounts for security risks in HAZMAT transport decision making (Macharis, Van Raemdonck et al. 2012).

5.3 Goal Programming

Goal programming belongs to the set of multi-criteria decision making (MCDM) techniques, and is one of the first techniques developed for decision making situations where conflicting goals cannot all be met simultaneously. Goal programming was first introduced by Charnes and Cooper (Charnes and Cooper 1961). Their work was at this point an extention of the linear programming methodologies first brought to light by George B. Dantzig in the 1940's, whose applications were military-specific. Multi-objective mathematical programming started with work of Koopmans (1951) in his work on activity analysis. A major contribution of his work was the identification of a non-

dominated vector, or an efficient vector, a concept that was used by Markowitz for his work on portfolio selection. The mathematical concept that provides the foundation of goal programming is first given in an article by Charnes, Cooper and Ferguson (Charnes, Cooper et al. 1955), where the authors minimize the sum of absolute deviations for a compensation decision problem. The groundwork for further applications of the GP method was laid out in later work (Charnes, Cooper et al. 1963).

There are at least 12 variations of goal programming, with the most common being weighted GP and lexicographical GP (Romero 1991, Aouni and Kettani 2001).[25] In weighted GP, the deviations from the goals are assigned weights based on the preferences and values of the decision maker, and the weighted sum of the deviations is minimized in the objective function. In Lexicographical GP, the goals are prioritized, so that those with greater priority are met with the least deviation from the goal before those objectives of a lesser priority are considered. Applications for GP have been extensively researched since the publication of this methodology, and have especially been developed within the fields of operations research.

The main advantage of using a GP approach as a multiple-criteria decision making tool is the ability to incorporate several conflicting goals within a single optimization function, and therefore the approach lends itself to finding a solution for logistics problems, which by nature require several trade-offs to be made. In this framework, costs are held to a target value, at the same time as target values for other factors are strived for. Therefore, the GP model inherently makes trade-offs between several decision variables for any given alternative. The values for the decision variables are constrained by the target values of the other decision variables, as well as system constraints.

5.3.1 Formulation of the GP Model

A goal programming model is a representation of a decision making situation in an organization, where multiple conflicting goals exist. A GP model has an objective function that seeks to minimize the sum of deviations of certain objectives from

[25] Variations of GP include: Integer GP, Nonlinear GP, Stochastic GP, Fractional GP, Interactive GP, Range and Interval GP, Fuzzy GP, MINMAX GP, Chance-constrained GP, GP and Constrained Regression.

corresponding target values, where, due to constraints, not all of the goals may be achieved simultaneously. An objective is the minimization or maximization of a decision attribute, such as risk, or profit, and is represented by a mathematical function: Max (f(x)) or Min (f(x)), where f(x) is a function of the decision attribute. Attributes, or characteristics, are defined as: "descriptors of reality" (Zeleny 1982).

A target is "an acceptable level of achievement for any of the attributes considered by the decision maker" (Romero 1991). A goal, then, is the combination of the target and the attribute. Deviations are underachievement or overachievement of the goals, while achievement of the goals can be easily determined using the target as reference point. Constraints of the system may disallow one or the other of these types of deviations. For example, in a short-term production scheduling problem, capacity is a constraint that disallows positive deviations in excess of capacity constraints.

Objectives differ from goals in that the former seek to maximize or minimize the level of a specific attribute or attributes, so that these can only be defined given a finite set of alternatives (Zeleny 1982). Goals, on the other hand, are specific and independent of the alternatives. Moreover, the achievement of goals can be evaluated by comparison with a reference stated *a priori*.

5.3.2 Critique of GP

Some of the technical limitations of GP were pointed out by Zeleney (1982), including the inherent capability of producing dominated, or non-Pareto efficient solutions, that the pre-emptive weighting approach is incompatible with utility preferences, and that the method fails to identify unbounded solutions (Zeleny 1982). These points for criticisms of GP are shown to be related to poor or inappropriate modelling practices, and can be overcome by applying more suitable modelling practices (Romero 1991). Moreover tests for efficiency and for appropriateness of solutions can be used to evaluate the generated solutions for suitability.

5.4 GP Model Formulation

5.4.1 Model Overview

In order to examine the effects of security on mode choice, a model is constructed of a simple network in which consignments must be picked up and delivered to a port location. The network consists of a warehouse (**Location L**), from which shipping consignments are picked up, a consolidation centre **(CC)**, where consignments might or might not be collected into full truckloads, an intermodal terminal (**Terminal**) where consignments are loaded onto either a train or barge, and a port, to which consignments are delivered by full truckload (**FTL)**, less-than-full truckload (**LFT**), inland waterway (**barge**), or train (**rail**), to the port (**Port**) There are multiple routes between the warehouse and the port. Transport modes road, rail and inland navigation are considered, but in the case of the latter two options, transhipment is required, whereas consolidation for road transport is optional.

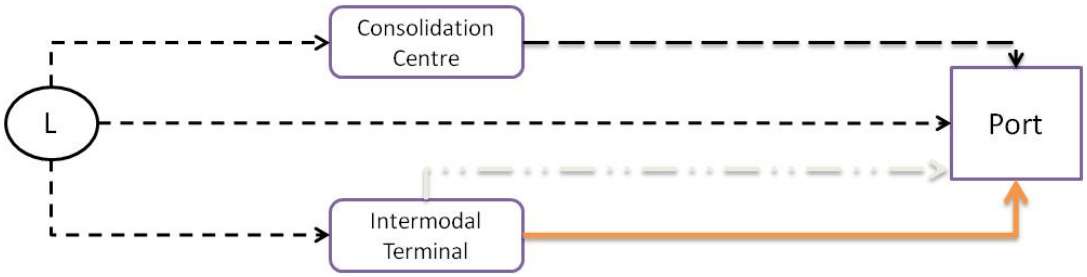

Figure 5.1 Simple Warehouse Network

The transport modes can be generalized, then, as decision alternatives, to which attribute measurements can be assigned. The attributes that are considered explicitly in the model are the direct transport costs, reliability of arrival time, loss through theft and damage, flexibility (that is, the minimum time required before a consignment can be booked), and travel time.

The goal program objective function minimizes total transport cost, early and late arrival times of shipments, as well as loss and damage (theft) of the consignments.[26] The approach inherently makes trade-offs between costs, flexibility, reliability, damage and

[26] The model accounts for the changes to costs, reliability, flexibility, transport time, damage and theft of transport that result from the implementation of security measures.

loss, security risk, and transport time in deciding to take a specific modal route (see Chapter 4) between a warehouse and the port, to which the goods must be transported.

A logistics service provider is assumed as the decision maker (Macharis, Pekin et al. 2008). The model looks only at inland transportation modes, and excludes the short-sea and over-sea shipping as well as air freight carriage.

Three scenarios are considered; the first is the status quo prior to the security regulations, the second reflects security factors for the decision environment (Dullaert, Vernimmen et al. 2007), to see if the selection of transport mode change, from the previous configuration, and the third looks at the configuration with an achieved AEO status. For each other three scenarios the parameters reflect changes in costs, transport time and transport time variability, flexibility, and loss and damage rates. The mathematical formulation of the GP mode choice problem is detailed below. The method was programmed in GAMS and solved with the CPLEX MIN solver.

5.4.2 Notations

Indices

i	origin location
j	destination location
d	origin, destination location
k; l	mode used
ijk	origin-destination-mode combination
c	consignments

Sets

I; J	Set of all locations
K	Set of transport modes
CO	matrix of consignment-origincombinations
CD	matrix of consignment-destination combinations

IJK origin-destination-mode matrix (route matrix)

C Consignments

Parameters:

Consignment Parameters

S_c Shipment size, in ton

ED_c Earliest consignment delivery time, in hours

LD_c Latest consignment delivery time, in hours

DT_c Desired consignment delivery time, in hours

IT_c Provision date when consignment is ready for shipment at origin, in hours

SR_c Estimated security risk of consignment (scale 1 to 5 of low to high perceived risk)

Route Matrix Parameters

CAP_{ijk} Capacity of mode *k* between two nodes *i* and *j*, in tonnes

FR_{ijk} Freight Rate, measured in €/tonne

TT_{ijk} Transport time, measured in hrs

Pen_{ijk} Security penalty (added cost for rests on link *k* between locations *i* and *j*)

Mode Parameters

UDT_k Unloading time of mode *k*

LDT_k Loading time of mode *k*

Location Parameters

SP_i Security penalty representing expected risk for rests at unsecured location *i*

Goal achievement Parameters

w_1 relative weight of shipment costs

w_2 relative weight of transit time reliability (both early and late arrival times)

w_3 relative weight of loss and damage rates

5.4.3 Assumptions

Following the findings of researchers in mode choice determinants, the attributes of the modes that are taken into consideration are:

- Flexibility
- Reliability
- Damage/loss (including theft)
- Security risk (relating to the value of the goods themselves, e.g., on the grey market, as in the case of high technology products)
- Cost (including freight rates, additional expenses and other related costs)
- Transit time (including delays, loading, unloading and groupage time)

The author proposes that security measures impact the utility of the attributes of the transport modes in the areas of: damage to goods, transit and handling times, theft, security risks, and costs (direct costs, as in carrying costs, investments; and indirect costs, e.g., personnel costs). The assumptions are described below.

Flexibility

Flexibility, also called notice or order time, is often defines as the time required between booking the shipment of a consignment and the point in time when the consignment is picked up. In some cases, as in rail, this could take up to 6 months for the advanced booking required by rail carriers (Crainic, Kim et al. 2007). This is, however, outside of the time frame of the model. Instead, flexibility is reduced to the amount of time spent at terminals before the consignment is underway again, which reflects the scheduled time windows that are a reality in the transport industry, especially in transport by barge or rail carrier and in the case of consolidations of road freight. Moreover, the minimum time between arranging for a shipment destined for the US is more than 24

hours, since a ship's manifest has to be sent to US customs 24 hours before the ship leaves the foreign port.[27] The model makes the following assumption:

- Security measures lower the flexibility, meaning that notice of a shipment has to be made farther in advance.

Reliability

Reliability of the delivery times is measured based on both late and early deliveries, since the latter result in undesired storage costs, or in the case of JIT manufacturing, can lead to backlogs in the queuing process. Not only are the deviations from expected delivery times considered, but also the magnitude of the deviations is important, especially for time-sensitive production systems. In logistics transport, delays can occur on any transport mode and are considered foreseeable on road, rail and inland waterway routes due to heavy traffic, scheduling and switching problems and water depth in canals, respectively. Besides reliability of actual transport times, transhipment, sorting and consolidating operations at terminals can affect the arrival time of containers. The model suppresses both late and early deliveries, but for the sake of simplicity, travel times for the different modes are given, and are assumed to be average transport times. Moreover loading and unloading times at the terminals are assumed. However, delays due to security measures are considered. Reliability is affected by security measures: longer waiting times at ports, etc., resulting in longer and variable lead times (Sheffi 2001, Voss, Closs et al. 2009). A probability is generated for delays for inspections. Other studies into the benefits of security measures have found that reliability of delivery times has been increased to as much as a 12 percent increase in on-time delivery (Peleg-Gillai, Bhat et al. 2006). The following assumption is therefore made for reliability of delivery times:

- Security measures increases the reliability of delivery times, in situation where the shipper/carrier is an AEO (Authorized Economic Operator), but decrease

[27] Cargo travelling unaccompanied by the proper documentation and information on these goods causes inefficiencies in the handling of the cargo, and represents a risk in safety and security Hauge, J. B., V. Boschian and P. Pagenelli (2009). Synchronisation of material and information flows in intermodal freight transport- an industrial case study. Dynamics in Logistics, Second International Conference, LDIC 2009, Preproceedings. Bremen, Germany, August 17 - 21, 2009..

reliability in other cases. That is, the magnitude of late deliveries increases if the operator is not an AEO operator.

Loss and Damage and Consignment Security Risk

Loss and damage is another important determinant of mode choice, also referred to as safety and security (Witlox and Vandaele 2005). Regarding the use of the shipping container as a means to minimize losses and damage to goods, as stated by Crainic et al.: "The initial impulse to container-based transportation came from the safety it offered regarding loss and damage" (Crainic, Kim et al. 2007). From a supply chain management perspective, the total cost and risk caused by loss and damage of freight is difficult to quantify, as it is greater than the value than the goods. The indirect costs due to loss and damage are those costs for stock-outs, backlogged inventory, and less quantifiable costs of not meeting service levels, making a given supply chain as a whole less competitive against a supply chain that is able to meet demand. The likelihood of theft in transport is high, specifically for high-value, low-volume goods, resulting in losses. Also, the likelihood of loss through damage and misplacement increases with every loading, unloading and transfer of the goods. Every occurrence of loss or damage in transport implies a concrete diminishment of the value of the goods (Witlox 2003). Security measures, however, provide a means of improving goods handling through automation, and thereby reducing opportunities for damage (Peleg-Gillai, Bhat et al. 2006).

In the model, loss and damage is the result of a combined probability of losses through theft or damage. The probability of loss and damage is specific for every chosen link or node given the transport mode or position in the network, and is therefore higher for some links and nodes than others. Moreover, security of the freight during transport requires that unless the freight is physical moving, it needs to be stored in areas where physical access to the goods is limited to authorized personnel. The model assumes that vulnerabilities for security breaches occur while the consignment is at rest in unsecured locations.[28] As a

[28] "Supply chain assets are more vulnerable when sitting still, such as at a service provider's warehouse, or while under the control of a transportation service provider (Gulisano, 2003)". Whipple, J. M., M. D. Voss and D. J. Closs (2009). "Supply chain security practices in the food industry: Do firms operating globally

result, security penalties are assigned to the consignment when it is at rest, either in storage, or delays in-transit. In-transit delays causing a consignment to be at rest for a period of time outside of a secured facility are penalized, but these vary depending on the link being used. Furthermore, as security risk is assigned to each consignment on a scale of 1 to 5, 1 being low and 5 being high, representing the attractiveness of the shipment for theft or tampering, such as in the case of high-value goods or supplies in disaster situations (Baldini, Oliveri et al. 2012). If the consignment is being stored at a certified facility, however, no security penalty occurs for the duration of the consignment's stay. This reflects findings that security measures have been shown to decrease pilferage by more than 30 percent (Peleg-Gillai, Bhat et al. 2006).

The following assumptions for loss and damage rates (as a function of delays and unsecured rest times, the risk levels assigned to consignments, and change-of-hands) are made in the model:

- Security measures decrease the theft and loss rates, reflecting the improvement in information flows and improvements to facilities and transport units to limit access to the goods.
- Freight delayed in transit or at unsecured storage sites result in penalties
- AEO status assumes that containers are locked and sealed with an e-seal, and the changes that the consignment is monitored is higher, resulting in few opportunities for tampering, and therefore the security penalties for transport time delays decrease

For the sake of simplicity, the model takes into account only direct losses, and not the indirect costs of lost sales, lower service levels, etc. Insurance coverage is also excluded.

Transport Times

Transport times are generally assumed to be within a fixed range for a given modal link between any nodes in the network. Time constraints result from requirements of the

---

and domestically differ?" International Journal of Physical Distribution & Logistics Management **39**(7): 574 - 594.

shipper as well as from the port operator. In the model these are reflected in earliest pick-up times from the warehouse locations and latest arrival times at the port. Travel time is also restricted due to port operations requiring latest possible arrival times. Where transport is done according to predefined schedules for these transport to get to a full-asset utilization, which is often the case in rail and inland waterway transport, the waiting time for the next scheduled is included in the assumed transport time.

- Transport time variations greater for shipping than for trucking services (Crainic, Kim et al. 2007)

Assuming scheduled transport exists for all rail and inland waterway, a waiting time is assumed for rail and waterway of 6 hours and 12 hours, respectively. In the post-9/11 scenario with mandatory security measures, however, it is assumed that additional precautionary measures are taken, such as visual inspections and verification of documents, and these lengthen the transit time. Where AEO status exists, it is assumed that these measures are redundant, so that the loading and unloading time actually decreases, as some manual checking is avoided through automation. So, where the operator has implemented security measures, transit time actually decreases, as was found by Peleg-Gillai et al (2006).

- Security measures lengthen the transhipment times (loading and unloading times measured in hours) – except for known shippers, AEOs, reflecting requirements at terminals that require additional goods sorting (for example, of dangerous goods) and verifications of documents and container seals.

Transport Costs

Transport costs are based on freight rates, which are calculated based on size of shipment (in tonnes). Fixed costs become more significant when security measures are taken into consideration, as some additional costs arise. To simplify the model, however, the freight rates are adjusted up to include the security-related costs. Moreover the increase in freight rate is based on the mode, as the findings in Chapter 2 show that some

portions of transport systems are more difficult to secure than others, specifically related to physical access security.

- Security measures increase costs (personnel, technology, procedural). Specifically, these costs depend of the position in the transport network (see 2.3 Impacts of Security Measures on Supply Chains).

In sum, the "service levels" provided by the modes change when security becomes incorporated in the model for determination of mode choice. However, whether the service level increase or decrease depends greatly on the utility function of the shipper, which is again dependent on the industry/product being shipped, and the type of supply chain (production/inventory) policy the shipper is acting under. In general, where the utility function of the shipper remains constant (a short-term assumption), the attribute function of the different modes will change, and therefore the alternative is evaluated differently.

For the model, each consignment is assigned a delivery window (in hours), with specified earliest, expected and latest possible delivery times. For each consignment there is also an attached level of risk, which reflects the nature of the goods.

5.4.4 Decision Variables

The model is in effect a route planning model, and so the decision variables X are binary, indicting if a route between nodes i and j is used.

X_{ijk} 1 if mode k between nodes i,j is used, O otherwise

The arrival time of a consignment is also assigned by the model. This allows for variances in the transport time and flexibility in delivery time and assigned delays.

AT_{cj} Arrival time of consignment c, at location j in hours

Accordingly, these variances of transport time and rest times, referred to from now on as buffer times, are assigned by the model, and represent any unforeseen delays or slack in the transport time and resting times that the consignment undertakes along its route. There are two kinds of buffer times assigned by the model: transit time buffers, for the time the

consignment is en route, and rest time buffers, for when the consignment is sitting at a terminal. The model assumes that no slack time appears between loading and leaving a location, that is to say, time spent a terminal is spend in the pre-loading area, and not on board. The buffer time are represented in the model by:

BTT_{cijk} Delays in travel time, or transport time buffers, for consignment *c* between nodes *i* and *j* over mode *k*, measured in hours

BTL_{ci} Slack time, or time buffer, for consignment *c* at location *i*, measured in hours

Losses and damage are also calculated by the model, and are represented as a percent of the shipment size lost over the course of the consignment's route. A random variable for loss and damages is generated for every route segment and at every node. The chances of loss and damage decline as security measures are taken in the system. The goal of the ratio of safe and usable goods upon arrival at the destination (the port, in this case), is 100%.

LD_c Loss and Damage, measured as percent of loss upon arrival.

In keeping with the formulation of the GP, additional decision variables are required. These allow for deviations from the target values of attributes, and inherently allow the model to make trade-offs between goal attainments of the various attributes to optimize the solution given the weights given to the target values of the attributes. In the given GP model, target values are assigned to the attributes cost and reliability.

d_1^+ Positive deviational variable of costs

d_2^+ Positive deviational variable of reliability, representing hours delivered late

d_2^- Negative deviational variable of reliability, representing hours under time

d_3^+ Positive deviational variable of loss and damage, representing shrinkage of the consignment

5.4.5 Goals and Objective Function

The goal program minimizes total transport cost, delayed and early shipments, and losses to the goods due to theft or damage. Therefore, the objective function (1) minimizes the weighted sum of freight cost, late and early deliveries, and loss and damage (theft) rates.

$$Min\ z = w_1 \sum_{c \in C} d_1^+ + w_2 \sum_{c \in C} d_2^+ + w_2 \sum_{c \in C} d_2^- + w_3 \sum_{c \in C} d_3^+ \quad (1)$$

5.4.6 Constraints

The total cost of shipping consignments is calculated by goal constraint (2), measured in freight rates, and dependant on the consignment size and mode selection.

$$\sum_{ijk \in IJK} FR_{ijk} \cdot S_c \cdot X_{cijk} - d_1^+ = 0 \quad \forall c \in C \quad (2)$$

Goal constraint (3) calculates late deliveries (measured in hours).

$$\sum_{c \in C} \sum_{i \in I} AT_{ci} - DT_c - d_2^+ + d_2^- = 0 \quad \forall ci \in CD \quad (3)$$

Goal constraint (4) calculates loss and damage and security penalties for the constraints (measured in tonnes):

$$\sum_{k,ijk \in IJK} X_{cijk} \cdot LD_{ijk} \cdot S_c + \sum_{k,ijk \in IJK} + BTT_{cijk} \cdot Pen_{ijk} \cdot SR_c \cdot S_c + \sum_{c \in C} \sum_{i \in I} BTL_{ci} \cdot PenN_i \cdot SR_c \cdot S_c - d_3^+ <= 0 \quad \forall c \in C \quad (4)$$

Goal constraint (5) holds early delivery time to zero.

$$\sum_{c \in C} \sum_{i \in I} AT_{ci} >= DT_c \quad \forall ci \in CD \quad (5)$$

Flow constraint (6) ensures that all consignments are picked up from their origin.

$$\sum_{j\in J}\sum_{k\in K} X_{cijk} = 1 \quad \forall ci \in CO \tag{6}$$

Flow constraint (7) ensures that all consignments coming into a location leave the location, as long as that location is not their destination.

$$\sum_{i\in I}\sum_{idk\in IJK} X_{cidk} = \sum_{j\in J}\sum_{djk\in IJK} X_{cdjk} \quad \forall cd \notin C0, cd \notin CD \tag{7}$$

Flow constraint (8) ensures that all consignments picked up arrive at their destination location (at the port).

$$\sum_{i\in I}\sum_{k\in IJK} X_{cijk} = 1 \quad \forall cj \in CD \tag{8}$$

Flow constraint (9) calculates the arrival time of consignment *c* at location *i* (is equal to its arrival time at the previous location *i*, plus the travel time between locations *i* and *j*, plus unloading time loading time.

$$\begin{aligned} &AT_{ci} + \sum_{k,ijk\in IJK} X_{cijk} * (LDT_k + TTijk + UDT_k) \leq \\ &AT_{cj} + (2 - \sum_{dik\in IJK} X_{cdik} - \sum_{l,ijl\in IJK} X_{cijk})M \quad \forall ij \in IJ, \forall cj \notin CD \end{aligned} \tag{9}$$

Time constraint (10) calculates the arrival time of consignment *c* at location *j* for consignments leaving their origin node.

$$\begin{aligned} &AT_{ci} + IT_c + \sum_{k,ijk\in IJK} X_{cijk} * (LDT_k + TTijk + UDT_k) \leq AT_{cj} \\ &+ (1 - \sum_{ijl\in IJK} X_{cijl})M \quad \forall ij \in IJ, \forall cj \notin CO, \forall ci \in CO \end{aligned} \tag{10}$$

Flow constraint (11) states that a consignment *c* travelling between locations *i* and *j* can travel by only one (available) mode between these two locations.

$$\sum_{k,ijk\in IJK} X_{cijk} \leq 1 \quad \forall c \in C, \forall i \in I, \forall j \in J \tag{11}$$

System constraint (12) represents the capacity constraint on route *IJK*.

$$S_c \cdot X_{cijk} \leq CAP_{ijk} \quad \forall c \in C, \forall ijk \in IJK \tag{12}$$

Flow constraint (13) ensures that arrival time of consignment *c* at unvisited locations is zero.

$$AT_{ci} \leq \sum_{j \in J} \sum_{k \in K} X_{cijk} \cdot M \quad \forall c \in C, \forall i \in I, \forall ijk \in IJK \tag{13}$$

Flow constraint (14) ensures that slack in travel time for consignment *c* may only be assigned to routes *ijk* travelled by consignment *c*.

$$BTT_{cijk} \leq X_{cijk} \cdot M \quad \forall c \in C, \forall ijk \in IJK \tag{14}$$

Flow constraint (15) ensures that slack in time spent at location *i* by consignment *c* may only be assigned if consignment *c* travels over location *i*.

$$BTL_{ci} \leq \sum_{j \in J} \sum_{k \in K} X_{cijk} \cdot M \quad \forall c \in C, \forall i \in I, \forall ijk \in IJK \tag{15}$$

Flow constraint (16) assigns slack time/delays for consignment *c* at locations *i* and routes *ijk* visited by consignment *c*, not including origin location and routes from the origin location.

$$\begin{aligned} &AT_{cj} - AT_{ci} - \sum_{k,ijk \in IJK} X_{cijk} \cdot LDT_k + TT_{ijk} + UDT_k - BTL_{ci} \leq \\ &\sum_{k,ijk \in IJK} BTT_{cijk} + (2 - \sum_{d} \sum_{k,dik \in IJK} X_{cdik} - \sum_{l,ijl \in IJK} X_{cdik}) \cdot M \quad \forall ij \in IJ, \forall cj \notin CO \end{aligned} \tag{16}$$

Flow constraint (17) assigns slack time/delays for consignment *c* at origin location *i* and on route *ijk* visited by consignment *c* from origin location c.

$$\begin{aligned} &AT_{cj} - AT_{ci} - IT_c - \sum_{k,ijk \in IJK} X_{cijk} \cdot (LDT_k + TT_{ijk} + UDT_k) \leq \\ &\sum_{k \in K} BTT_{cijk} + (1 - \sum_{l,ijl \in IJK} X_{cijl}) \cdot M \quad \forall ij \in IJ, \forall cj \notin CD, \forall ci \in CO \end{aligned} \tag{17}$$

5.5 Parameters for Scenarios

The transportation decision is modelling the movement of consignments between a shipper's warehouse location and a port location along a network of alternative modal routes, where the selection is not made between the routes but between the transport modes (see Figure 5.1). Assumptions are made for freight rates and security costs, transport times (travel times and times for transhipment), as well as order time in three different scenarios. The parameters shift in each scenario to reflect security factors for the decision environment (Dullaert, Vernimmen et al. 2007), to see if the selection of transport mode changes, from the previous configuration.

This section defines the context of the modal choice decision in terms of strategic level, reference units, and the composites for the cost and time functions and calculations of losses that are used in the model.

It is assumed that the port is secured in compliance with ISPS regulations, and the intermodal terminal is an equally secure area according to TAPA rules. The originating warehouse and the consolidation centre are not secured.

5.5.1 Scenario 1 Pre-9/11

The first scenario typifies the mode choice model, where trade-offs are made between freight rates, transit time, and expected loss and damage rates. Flexibility is represented by the difference between the initial times when the consignments are available for pickup, and the next available shipment. The latest and earliest delivery times limit the non-goal achievement of the reliability goals to a range of arrival times of plus/minus 10% of the desired arrival time. Costs, losses and delays in the system are minimized.

Table 5.1 Scenario 1 Route Parameters

Transport Alternative	Freight Rate (€/tonne)	Transport Time (hr)	Security Penalty (per hr of delay)	Loss and Damage Rate
A_1 L to Port via LFT	1200	5	0.6951%	0.03
A_2 L to Terminal via LFT	600	1	0.1996%	0.03
A_3 Terminal to Port via FTL	360	8	4.7561%	0.05
A_4 Terminal to Port via Rail	240	8	0.0999%	0.02
A_5 Terminal to Port via Barge	156	15	0.4975%	0.02

Table 5.2 Scenario 1 Consignment Parameters

Consignment	Shipment Size (tonnes)	EDT	LDT	DDT	Initial Times	Security Risk
c1	50	203	248	226	0	5
c2	60	126	154	140	124	4
c3	70	58	71	65	51	3
c4	40	108	133	121	106	2
c5	50	73	90	82	71	1

Table 5.3 Scenario 1 Mode Parameters

Mode	Loading Time	Unloading Time
LFT	1	1
FTL	6	1
Train	6	6
Barge	12	6

Table 5.4 Scenario 1 Node Security Parameters

Node	Security Risk (per hour of stay)
Warehouse	0.099%
Terminal	0.399%
Port	0.299%

The security risks for losses through theft or damage to goods as well as unauthorized access to the goods are estimated using a Poisson distribution, and are multiplied by the number of hours that goods spend at rest.

5.5.2 Scenario 2 Post-9/11[29]

The same scenario is presented, with changes to the criteria parameters. The freight costs are higher, because the costs for security measures at ports are passed on through the transport chain and, ultimately, to the shipper. In actuality, a security fee is payable, for example a $ 40 levy is charged for all consignments at ports. For simplification, the freight rates were increased by 20 percent.

At least 24 hours must elapse between the ordering of the shipment and its arrival at the port, meaning that flexibility is reduced, which impacts road transport in particular. Furthermore, it is assumed that the documentation arrives at the port with the container, so that the consignment must remain at port for at least 24 hours.[30] Late arrivals are therefore not allowed in this scenario.

[29] "These results suggest that supply chain efficiency related benefits are the result of certain security measures which contribute to security and at the same time, create operationally desirable conditions that are essential for improving efficiency. For instance, some respondents explained that certain security measures reduced the time and variability of certain logistics operations and improved cargo visibility and control, which together contributed to the reduction of the vulnerability of the supply chain. Others reported an improvement in logistics processes and level of service, which contributed to the improvement of supply chain performance. In spite of these examples, which connect certain measures and benefits, there were several respondents who argued that the obtained benefits were the result of all the implemented measures and they were not able to establish any relevant connections between single measures and single benefits." Gutiérrez, X., J. Hintsa, P. Wieser and A.-P. Hameri (2007). "Voluntary Supply Chain Security Program Impacts: An Empirical Study with BASC Member Companies." World Customs Journal **Volume 1**(Issue 2).

[30] "The 24-h rule requires that liner companies and non-vessel operation common carriers provide the US government with a1-day advance notice of a container being loaded onto a vessel. It allows the US government to identify containers that require additional inspection before being shipped to an American port... The 24-h rule has significantly impacted the flexibility of loading ports and shippers by requiring information to be gathered and transmitted early in the booking cycle and inhibiting the ability to make last minute changes." Yang, Y.-C. (2011). "Risk management of Taiwan's maritime supply chain security." Safety Science **49**(3): 382-393.

Table 5.5 Scenario 2 Route Parameters

Route	Freight Rate (€/tonne)	Transport Time (hr)	Security Penalty (per hr of delay)	Loss and Damage Rate
A_1 L to Port via LFT	1100	5	0.6951%	0.03
A_2 L to Terminal via LFT	550	1	0.1996%	0.03
A_3 Terminal to Port via FTL	330	8	4.7561%	0.05
A_4 Terminal to Port via Rail	220	8	0.0999%	0.02
A_5 Terminal to Port via Barge	143	15	0.4975%	0.02

Table 5.6 Scenario 2 Consignment Parameters

Consignment	Shipment Size (tonne)	EDT	LDT	DDT	Initial Times	Security Risk
c1	50	0	202	226	0	5
c2	60	0	132	140	124	4
c3	70	0	61	65	51	3
c4	40	0	115	121	106	2
c5	50	0	84	82	71	1

Table 5.7 Scenario 2 Mode Parameters

Mode	Loading Time	Unloading Time
LFL	1.1	1.1
FTL	6.6	1.1
Train	6.6	6.6
Barge	13.2	6.6

Table 5.8 Scenario 2 Node Parameters

Node	Security Risk (per hour of stay)
Warehouse	0.199%
Terminal	0.099%
Port	0.199%

5.5.3 Scenario 3 AEO Status

Visibility, trust, and transparency are key to creating benefits when implementing security regulations, whether this is achieved through organizational and managerial changes, or technological ones.

In this scenario, the following scenario assumptions apply:

- the minimum time between the initial ordering of the consignment and its arrival at the port must be at least 24 hours (but there are no constraints made on how long the consignment can be delayed en route)
- Security penalties per hour for consignments stored at the warehouse is close to zero, since the risk of accessing these nodes in the network is low, due to new security measures. The security penalties for consignments residing at the intermodal terminal are higher because these terminals are more difficult to achieve the same level of access limitations, but are still lower than in the previous scenarios. The security penalties for delays en route are lower, to reflect the use of e-seals and track-and-trace technologies, which alert the LSP and the shipper when the consignment has been tampered with or opened.
- The flexibility of the shipments is lower; this is modelled by setting the earliest delivery time to at least 24 hours after the initial time. However, as it is assumed that as soon as the consignment can be picked up, the documentation is sent, meaning that the documentation precedes the shipment to the port, therefore no requirement is made for the container to remain there for the minimum 24-hour period.
- The freight rates are higher than in Scenario 2 to include the cost of certification, employee vetting, and investments into information systems that are required by the AEO status.

Table 5.9 Scenario 3 Route Parameters

Route	Freight Rate (€/tonne)	Transport Time (hr)	Security Penalty (per hr of delay)	Loss and Damage Rate
A_1 L to Port via LFT	1200	5	0.06951%	0.015
A_2 L to Terminal via LFT	600	1	0.01996%	0.015
A_3 Terminal to Port via FTL	300	8	0.01996%	0.025
A_4 Terminal to Port via Rail	240	8	0.00999%	0.010
A_5 Terminal to Port via Barge	156	15	0.0004975%	0.010

Table 5.10 Scenario 3 Consignment Parameters

Consignment	Shipment Size (tonne)	EDT	LDT	DDT	Initial Times	Security Risk (1-5)
c1	50	203	248	226	0	5
c2	60	148	154	140	124	4
c3	70	75	75	65	51	3
c4	40	130	133	121	106	2
c5	50	95	95	82	71	1

Table 5.11 Scenario 3 Mode Parameters

Mode	Loading Time	Unloading Time
LFL	0.8	0.8
FTL	4.8	0.8
Train	4.8	4.8
Barge	9.6	4.8

Table 5.12 Scenario 3 Node Security Parameters

Node	Security Risk (per hour of stay)
Warehouse	0.01%
Terminal	0.09%
Port	0.01%

5.6 Limitations of the Model

Some risk-related costs were not reflected in the model, including insurance costs and insurance pay-outs. More importantly, indirect costs of losses and damages to the consignments related to interrupted supply, such a lower service levels, stock-outs, and inventory backlog and hence total logistics costs, are not fully accounted for. The frame of reference of this model is a logistics service provider, so that only attributes of the transport function were taken into account, while changes in inventory and holding costs were ignored.[31] On the other hand, in assigning a freight rate based on shipment size, the model does account for economies of scale achieved through consolidation; in actuality, however, lower transport costs (FR) would result from a higher shipment volume. For future research, it would be interesting to further explicit consideration of total logistics costs not only as part of operational decision making, but also at the tactical and strategic levels, and towards a transportation policy. A further limiting aspect of the approach used in this thesis is the exclusion of any advantages of partnerships facilitated by technological advances, such as tracking and tracing technologies and indicators such as RFID-enabled e-seals. Furthermore, the model doesn't take into account in any real way the discrepancies the attractiveness of the goods for theft. Several factors could be mentioned here, most notably the value of the transports (measured in value/area or value/weight), especially important in high-tech products, or seasonality (such as children's toys in holiday seasons), or how easily the stolen goods could be sold on the black market (such as cigarettes, alcohol, brand-name apparel and high-tech goods). Ideally, the probability of shipments of more desirable goods being targeted would provide more accuracy for the weighting given to the L&D component of the objective function.

[31] The model would be more complete if the inventory and transport policy would be combined and observed from the perspective of the supply chain, especially considering that improved inventory policies and potential for lower overall goods along the supply chain due to lower theft, less instances of damage and loss through better handling systems, and shorter, more reliable delivery times are purported as major benefits resulting from implementing supply chain security measures Peleg-Gillai, B., G. Bhat and L. Sept (2006). Innovators in Supply Chain Security: Better Security Drives Business Value. The Manufacturing Innovation Series. T. M. Institute, Standford University..

5.7 Results

The GP model was used to evaluate the three scenarios described above.

Weight rankings for transport service factors are adapted from Witlox' listing of weight factors in mode choice: (Witlox, 2005).[32] These remain the same for each of the three scenarios listed above.

For all scenarios, the following weights for the optimization function were used:

Table 5.13 Weighing Parameters for Goal Attainment

Weights of Goal Attainment	
W_1 Costs	0.44
W_2 Reliability of arrival times	0.40
W_3 Loss and Damage	0.16

5.7.1 Scenario 1 Results

The model prefers to assign the consignments to barge or rail where time restrictions allow, which minimizes the costs and expected losses through damage or costs of the security penalty for en route delays that would occur when shipping by road transport. Where the weight of the reliability factor becomes larger, however, the goods are shipped over the intermodal terminal by FTL at higher costs. The total costs and performance measurements for arrival time reliability, loss and damage, flexibility, and travel time for the present weighted configuration is given in

Table 5.14.

Table 5.14 Scenario 1 Transport Assignment and Performance

Consignment	Transport Alternative	Cost (€)	Early Arrival (hrs)	Late Arrival (hrs)	Losses (tonne)
C1	A_1 LFL + A_4 Rail	37800		0	3.0
C2	A_1 LFL + A_5 Barge	35000		7	2.5
C3	A_1 LFL + A_3 FTL	49000		9	5.6

[32] Compare Vannieuwenhuyse, B., L. Gelders and L. Pintelon (2003). "An online decision support system for transportation mode choice." Logistics Information Management **16**(2): 125-133..

C4	**A_1 LFL + A_4 Rail**	32000		8	2.0
C5	**A_1 LFL + A_3 FTL**	35000		12	4.0
Total		188800	-	-	-

5.7.2 Scenario 2 Results

In this cost-sensitive scenario, the costs for shipments increase, and the goods are shipped by train as much as possible to avoid extra transport costs. This results in higher delays of shipments by between 12% and 20%, despite additional costs of 7.6%. The reduction in losses for the first consignment is a result of the smaller transport delay and therefore the security penalty for this chosen mode is lower. The model puts all consignments at the intermodal terminal for storage during time buffers to limit security risks. Costs and quality performance measures for the selected alternative for the scenario are given below.

Table 5.15 Scenario 2 Transport Assignment and Performance

Consignment	Transport Alternative	Cost (€)	Early Arrival (hrs)	Late Arrival (hrs)	Losses (tonne)
C1	A_1 LFT + A_4 FTL	41580			58.4
C2	A_1 LFT + A_5 Barge	38500		8.4	2.5
C3	A_1 LFT + A_3 FTL	53900		10.4	3.5
C4	A_1 LFT + A_4 Rail	30800		9.4	2.0
C5	A_1 LFT + A_3 FTL	38500		13.4	2.5
Total		203280	-	-	-

5.7.3 Scenario 3 Results

Under the AEO status scenario, the lower flexibility of the shipments is the main obstacle to achieving the desired arrival times. Late arrivals are forced by the system requiring at least 24 hours' notice before the shipment can be loaded onto a sea-going ship. The required extra time means that slack time is introduced into the system, and allows for shipments by train or barge rather than by the faster truck transport. The costs are increased over the first scenario by 14.3%, but these costs would be offset to a degree by the lower expected losses through theft and tampering en route, as well as increased efficiency of inventory policies due to better information preceding the goods. As the warehouse is secured, all slack time is assigned to this node in the model. This would be unrealistic if the exact scheduling of the train and barge transports were taken into account, however.

Table 5.16 Scenario 3 Transport Assignment and Performance

Consignment	Transport Alternative	Cost (€)	Early Arrival (hrs)	Late Arrival (hrs)	Losses (tonne)
C1	A_1 LFT + A_5 Barge	45360			2.1
C2	A_1 LFT + A_4 Rail	42000		8	1.3
C3	A_1 LFT + A_4 Rail	52920		18	1.8
C4	A_1 LFT + A_4 Rail	33600		9	1.0
C5	A_1 LFT + A_4 Rail	42000		13	1.3
Total		215880	-	-	-

5.8 Conclusions

A goal programming model was constructed for a transport mode assignment problem of a logistics service provider. The cost-service trade-offs involved in this decision situation were modelled, and the hypothetical problem was analysed in the context of new security regulations. The model requires earlier planning of shipments is required and as a consequence the flexibility of sea-bound consignments is lower. The model shows that the total cost of the transportation of the consignments has increased; these extra costs need to be offset by lower damage and reliability levels that are available through tighter security actions and the advantages that these can provide for inventory and sourcing policies at

the supply chain level. At the same time, there is a shift between the prior to and post-security regulations scenarios where road transport (per LTF, FTL) loses some of its favourability against rail and barge transport.

Chapter 6 Summary of Research Findings and Perspectives for Future Research in Supply Chain Security

This research set out to create a decision support tool for intermodal logistics with special consideration for supply chain security. The topic of supply chain security was explored as a major issue facing modern supply chains as well as a key area for research within supply chain management theory. The major security-related issues facing supply chains were discussed as well as the contributions of supply chain management literature towards these issues. Opportunities for logistics planning, in particular in intermodal transport planning, to improve security of supply chains were researched. Following this, management science approaches were looked at for suitability in building a decision support tool for intermodal planning in the context of high requirements for supply chain security. Finally, a goal programming model was built as such a decision support tool.

This chapter highlights major findings as outcomes of the work and offers perspectives on potential areas for future contributions in supply chain management security, in MCDM and towards government involvement in logistics security.

6.1 Major Research Findings

Supply chain security is a topic that has grown in importance over the last decade for the logistics industry as well as within academia. The significance of security for supply chains is due to: a) the pressure security regulations have put onto supply chains and particularly on logistics service providers, and b) the increased awareness of security risks, including those of terrorism, theft, and damage, and the potential in these risks for significant damages. Security risks involve not only the loss of assets through theft and counterfeit, but also the threat of man-made disaster through sabotage and terrorism, as well as smuggling involving transports.

The heightened perception of these security risks and the regulatory pressures enumerated above are major drivers for implementing security measures. Beyond the risk perception and security regulations are the institutionalization and expectations in the

transport industry of compliance and certification along regulatory frameworks, which act as drivers for security. Foremost of the reasons for implementing supply chain security measures, however, is the strategic importance of maintaining a trustworthy company image and corporate credibility. Supply chain security, then, is of strategic importance and is a necessary, though costly, part of doing business in the post 9/11 era.

In order to resolve the apparent conflict between the costs of supply chain security and the requirements for supply chain efficiency, three main goals of supply chain security, were found to include: a) achieving value through efficiencies in supply chain-related business processes; b) managing security risks; and c) to gain capabilities in detecting, responding to and recovering from unforeseen events and crises. The theory of supply chain management and several theoretical frameworks within supply chain management were looked to for potential means of achieving supply chain efficiencies as well as increased security through the implementation of security measures. In particular Quality Management, Risk Management and Crisis Management were examined for possible contributions towards the achievement of these three objectives, resulting in several key findings. First, because risks are inherent to supply chains and their processes, supply chain security is an organizational issue rather than merely a technical one, and secondly, because of the high level of interdependency between supply chain partners, achieving benefits through SCS is beyond the capabilities of any one organization, but requires collaboration between partners along the supply chain. Thirdly, mitigating security risks requires information sharing along the supply chain that contributes to its ability to detect and mitigate disaster, thereby making the supply chain less vulnerable to attack and more resilient in the case of a security event.

Based on these outcomes of supply chain theoretical approaches, five major categories of supply chain security measures have been identified, including: 1) tighter collaboration through improved communication and information sharing across the supply chain; 2) organizational compliance with government and industry-led security regulations; 3) the reorganization of logistics operations, such as the implementation of visibility technology and plans for alternative transportation and inventory processes; 4) building up of

flexibility and resilience towards business continuity; and finally, 5) fostering a security culture of organizations through training and knowledge sharing with the objectives of creating a competitive advantage through security capabilities and trust.

Logistics planning is one area of particular interest in investigating opportunities for increasing the security of supply chains. For one thing, the logistics sector is influenced more directly by security regulations than other sectors and bears a very significant portion of the costs of compliance. Logistics service providers in particular are under scrutiny. LSPs deal with greater requirements for security due to their role in cross-border transport operations, because of their integrated, operational function within the supply chain, and because of the pressure to be known as a "secure operator". Another important reason why logistics planning is an interesting point of study is because it is on the level of the physical assets, infrastructure and transport operations where security risks are most tangible. In particular transport networks play a vital role in the performance in cost and quality factors of transport operations; therefore, transport mode choice is a key variable in the efficiency and effectiveness of logistics operations. For this reason, the mode choice problem was explored as a key factor in securing operational supply chain transport activities.

A range of factors play a role in the mode choice decisions, the more significant of which include the contribution of the mode choice to total logistics costs and quality factors of the transport modes. The rising costs of transport is making alternate modes of freight more attractive over road carriage, particularly over large distances, meaning that intermodal transport is continuing to garner the interest of shippers as a viable alternative to keep costs down. Intermodal transport is also interesting as an alternative to road transport where security is an issue. The complexity of the trade-offs in cost and quality factors and additionally the consideration of security factors of the transport modes present a decision situation that can be supported through decision support.

Decision support models are developed based on operations research methodologies to facilitate the information gathering, analysis and evaluation tasks of decision making. Due to the organization-spanning nature of supply chains, OR models for supply chain and

logistics need to support decisions involving multiple actors, multiple conflicting objectives, and multiple decision criteria. A goal programming methodology was chosen for the mode choice selection tool because of its capability of taking multiple criteria, objectives and evaluation criteria into consideration. A GP model was therefore constructed to support trade-off decision-making. Three scenarios were tested with the model based on a hypothetical situation within a small transport network. The scenarios involved a transport mode choice decision: 1) where no security regulations exist, 2) in the presence of security regulations for cross-border transports, and 3) in the presence of cross-border transport security and compliance on the part of the LSP as a secure operator. The cost-quality trade-offs were made based on assumed changes in the costs and quality factors, as represented in the model parameters. The model demonstrated a) an increase in overall costs, and b) a decrease in the favourability of road transport over intermodal transport between the pre-security regulation and post-security regulation scenarios, respectively. Rail was favoured over barge where transit time was scarce.

6.2 Perspectives for Future Research in Supply Chain Security

The field of supply chain security is still relatively young, though it is attracting a great deal of interest. The main issue continues to be balancing the need to mitigate security risks while maintaining competitiveness through value creation, driving areas for potential gains in business process efficiency, security risk mitigation, and supply chain resiliency. However, the paths toward the achievement of these security objectives are still areas for potential research. Supply chain theoretical approaches for strategic direction and decision support for operational planning represent two main areas for future contribution to the topic. Over and above strategic and operational planning are issues relating to the future role of government in supply chain and logistic security, whether as a partner with industry in mitigating security risks or as a facilitator of international trade.

6.2.1 Supply Chain Management Approaches for Supply Chain Security

The interdisciplinary nature of the history of SCM as an area of study represents both a strength as well a stumbling block for the future development of SCM. SCM theory

incorporates perspectives from the strategic, tactical and operational planning levels as well as perspectives from across all organizational functions of business in the process of creating value. However, this has meant that the domain of the theory is not delineated for theory development as of yet (New 1997). Also problematic are the competing definitions of SCM. The common denominator of these definitions is the inter-organizational nature of SCM studies, although none of the disciplines that are fundamentals of SCM are able to provide the necessary analysis tools for the cross-organizational culture that exists in SCM (Macharis, Van Hoeck et al. 2010), and the challenges that managers face are therefore treated far more trivially than they really are in actuality. To demonstrate this issue, New points out that the concept of "partnership" often purported in the literature is not reflective of the relationships that exist between firms in supply chains (New 1997). For example, risk-sharing along the supply chain is an idealized version of the in-actuality extant risk-shifting by more dominant players in the supply chain unto firms that are less able to bear them that takes place in the industry. [33]

Recent work in supply chain security has brought this topic to the forefront. Significant contributions were made within the topic, specifically towards theoretically-based solutions to the problems of finding efficiencies out of supply chain security measures. While the drivers for supply chain security are clear, however, they are not yet linked to the strategy of organizations and of supply chains; moreover, the concept of supply chain security is only currently being operationalized (Gould 2010). Until this is done, there remains a difficulty in incorporating security constructs in planning models. And finally, because of the interorganizational nature of supply chains, improving their resilience requires collaboration and information sharing that is beyond what is the norm between

[33] Lindroth and Norrman Lindroth, R. and A. Norrman (2001). Supply Chain Risk and Risk Sharing Instruments - An Illustration from the Telecommunication Industry. Proceedings of the Logistics Research Network 6th Annual Conference, September 13-14, 2001. L. R. Network. Heriot-Watt University, Institute of Logistics and Transport**:** 297-307. found that models for risk and reward sharing in the supply chain are scarce in the literature. They cite the works of Mentzer and Lambert and Cooper as a couple of the fewer contributions to this area: "Mentzer (2001) and Lambert and Cooper (2000) found sharing risks and rewards across the SC to be a key component of supply chain management." Norrman, A. and U. Jansson (2004). "Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident." International Journal of Physical Distribution & Logistics Management **34**(5): 434 - 456..

actors, namely the provision of real-time information as well as policies for decision making in real time for effective response.

Specific to the objectives of supply chain security outlined in this work, problem areas for future research in supply chain management include:

1. Linking operational security to supply chain strategy, including the incorporation of meaningful security constructs in planning;

2. Integration of real-time, event-driven data and information in planning, and relatedly;

3. Non-hierarchical planning in the context of conflicting goals, high complexity and dynamicity; and finally

4. Providing increasingly meaningful and applicable frameworks for organizational integration.

6.2.2 Decision Support and Model Building for Operational Supply Chain Security

As much as operations research has contributed to the area of logistics and transport planning (see Chapter 4), certain characteristics of the traditional forms of modelling limit their applicability for the complexities of intermodal transportation planning problems going forward. For one thing, OR models and methodologies are complex and not easily understood, let along applied, by managers who are their target users; the models therefore do not accurately reflect the perception of transportation policy makers and users (van Duin and van Ham 1998). For another, models have focussed in the past on a single decision maker or on a specific planning horizon (long term strategic vs. short-term operational planning) without explicitly accounting for the interdependencies of these planning levels. Lastly, the quantitative nature of these models makes it difficult to incorporate qualitative factors. These issues impact the usefulness of decision support

models in supporting organizations and inter-organizational supply chains in decision making towards their strategic goals.

> *...Of course, it is almost impossible to develop a general single model that integrates all these aspects. The conclusion leads to the development of an overall methodological transportation framework, supported by multiple interrelated models capable of representing qualitative factors and uncertainties. The development of* ***an*** *approach to build these interrelation models must fill the gap between logistic decision processes on the one hand, and the specification of the design contents on the other hand. The new models must be easy to use and understand, with user-friendly capabilities, such as graphical representations of the systems under analysis.* (van Duin and van Ham 1998)

The work of van Duin and van Ham point to the requirement that models be able to look at the decision framework outside of and beyond the scope of a single firm, and incorporate factors from the environment. This is very important for the decision environment that exists in supply chains, which are complex networks showing mutual interdependencies. The decision setting is neither hierarchical nor market oriented, but requires cooperation and collaboration. This has the potential to lead to newer methods of control (such as autonomous cooperation); in any case, co-ordinating structures in a multi-actor chain represent an area for future research (Bontekoning, Macharis et al. 2004), especially those incorporating multiple actors and multiple planning horizons (Macharis, Van Raemdonck et al. 2012). In sum, future research is challenged to address these issues by:

1. Forwarding modelling methodologies that are closer to the perception of transport policy makers, transport operators and users;
2. Incorporating multiple actors and multiple levels of planning in meaningful ways;
3. Incorporating qualitative factors in transport planning to support the goals of the supply chains using the transport activities. Some relevant qualitative factors for

further research relating to supply chain security include: a) trust between the shipper and the transport operators and b) security capabilities resulting from characteristics such as security culture, presence and use of forewarning mechanisms, and contingency and continuity planning.

6.2.3 Changing Role of Government: Facilitators of Secure Trade

Regulatory bodies, customs agencies and governments are increasingly seeing their role and taking up a position in security of supply chains as a facilitator of secure trade (INTEGRITY and SMART-CM 2008). Prior to this, the government's role related to protectionism and collection of customs. Interdiction of transport across national borders targeted illegal persons and illicit goods (narcotics, contraband). Protection against the threat of terrorism is the new perspective. Considering the risk of loss of life and the potential costs in the case of destruction of critical infrastructure, customs bodies and security regulations are moving away from their previous role as controllers and shifting to contributors of national security and ensuring security as a *public good*. The political security of a region is also a major evaluation criterion for investment into a logistics zones (Lu and Yang 2007). The relative security of a region, meaning lower average costs for logistics security, can even contribute the competitiveness of that region. This means a more active role for regulatory bodies in the logistics industry: that of an invested partner in the transport chain, and an active contributor to value creation (Hameri and Hintsa 2009). Public-private partnership is a byword for this role.

Some major questions arise: from the perspective of the supply chain, what role can the government have as a partner in a supply chain? How can a public-private partnership contribute positively to supply chain performance regarding SCS (Williams, Lueg et al. 2009)? It was shown that governmental regulations have increased costs of doing business for supply chain processes and even present artificial barriers to trade (Grainger 2007), but in what ways can public policy support efficiencies between security and supply chain performance? A Delphi-study by Hameri and Hintsa identified collaboration between business and government actors to be a success factor for future supply chains; the interface between trade and customs is one key area that will shape relationship

management between customs and trade (Hameri and Hintsa 2009).

6.3 Final Remarks

In a world that continues to become increasingly globalized, supply chain processes find themselves at the heart of shifting production and distribution processes. At the same time logistics processes will be a source of the future flexibility of production and distribution systems. New capabilities in management and decision making will also have to evolve in order to cope with such changes. Understanding how to build these capabilities will provide a host of opportunities for future contributions.

References

A. T. Kearney. (2005). "Smart Boxes." Retrieved 20.01.2010, from http://www.atkearney.com/index.php/Publications/smart-boxes.html

Adams, H. W., Ed. (1992). Unternehmerisches Risikomanagement: bessere Organisation - mehr Sicherheit, Verl. TÜV Rheinland.

Akkermans, H., P. Bogerd and J. van Doremalen (2004). "Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics." European Journal of Operational Research **153**(2): 445-456.

Altay, N. and W. G. Green, III (2006). "OR/MS research in disaster operations management." European Journal of Operational Research **175**(1): 475-493.

Aouni, B. and O. Kettani (2001). "Goal programming model: A glorious history and a promising future." European Journal of Operational Research **133**(2): 225-231.

Autry, C. W. and L. M. Bobbitt (2008). "Supply chain security orientation: conceptual development and a proposed framework." The International Journal of Logistics Management **19**(1): 42 - 64.

Badea, A. C., C. M. Rocco S, S. Tarantola and R. Bolado (2011). "Composite indicators for security of energy supply using ordered weighted averaging." Reliability Engineering & System Safety **96**(6): 651-662.

Baldini, G., F. Oliveri, M. Braun, H. Seuschek and E. Hess (2012). "Securing disaster supply chains with cryptography enhanced RFID." Disaster Prevention and Management **21**(1): 51-70.

Ballou, R. H. (1999). Business logistic's management : planning, organizing, and controlling the supply chain. London, Prentice-Hall International.

Bandyopadhyay, T., V. Jacob and S. Raghunathan (2010). "Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest." Information Technology and Management **11**(1): 7-23.

Banister, D. and J. Berechman (2000). Transport investment and economic development. London, UCL Press.

Banomyong, R. (2005). "The impact of port and trade security initiatives on maritime supply-chain management." Maritime Policy & Management **32**(1): 3-13.

Barnes, P. and R. Oloruntoba (2005). "Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management." Journal of International Management **11**(4): 519-540.

Beamon, B. M. and T. M. Ware (1998). "A process quality model for the analysis, improvement and control of supply chain systems." International Journal of Physical Distribution & Logistics Management **28**(9/10): 704.

Bernasek, A. (2002). "The Friction Economy." Fortune **145**(4): 104-112.

Bichou, K. (2004). "The ISPS Code and The Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management." Maritime Economics and Logistics **6**(4): 322-348.

Bichou, K., L. Kee-Hung, Y. H. V. Lun and T. C. E. Cheng (2007). "A Quality Management Framework for Liner Shipping Companies to Implement the 24-Hour Advance Vessel Manifest Rule." Transportation Journal **46**(1): 5-21.

Bontekoning, Y. M., C. Macharis and J. J. Trip (2004). "Is a New Applied Transportation Research Field Emerging?--Review of Intermodal Rail-Truck Freight Transport Literature." Transportation Research: Part A: Policy and Practice **38 1**: 1-34.

Boote, D. N. and P. Beile (2005). "Scholars before Researchers: On the Centrality of the Dissertation Literature Review in Research Preparation." Educational Researcher **34**(6): 3-15.

Bottani, E. and A. Rizzi (2006). "A fuzzy TOPSIS methodology to support outsourcing of logistics services." Supply Chain Management: An International Journal **11**(4): 294 - 308.

Burgess, K. and P. J. Singh (2006). "A proposed integrated framework for analysing supply chains." Supply Chain Management: An International Journal **11**(4): 337 - 344.

Caramia, M. and F. Guerriero (2009). "A heuristic approach to long-haul freight transportation with multiple objective functions." Omega **37**(3): 600-614.

Caris, A. (2010). Simulation and Optimisation of Intermodal Barge Transport Networks, Universiteit Hasselt.

Caris, A., G. Janssens and C. Macharis (2009). Modelling Complex Intermodal Freight Flows
From System Complexity to Emergent Properties. M. Aziz-Alaoui and C. Bertelle, Springer Berlin / Heidelberg. **44:** 291-300.

Carluer, F. (2008). Global Logistic Chain Security: Economic Impacts of the 100% Container Scanning Law Brussels, WCO, World Customs Organization.

Cavinato, J. L. (2004). "Supply chain logistics risks: From the back room to the board room." International Journal of Physical Distribution & Logistics Management **34**(5): 383 - 387.

Charnes, A. and W. W. Cooper (1961). Management Models and Industrial Applications. New York, John Wiley & Sons.

Charnes, A., W. W. Cooper and R. O. Ferguson (1955). "Optimal Estimation of Executive Compensation by Linear Programming." Management Science **1**(2): 138-151.

Charnes, A., W. W. Cooper and Y. Ijiri (1963). "Breakeven Budgeting and Programming to Goals." Journal of Accounting Research **1**(1): 16-43.

Chen, I. J. and A. Paulraj (2004). "Towards a theory of supply chain management: the constructs and measurements." Journal of Operations Management **22**(2): 119-150.

Chopra, S. and M. S. Sodhi (2004). "Managing risk to avoid supply-chain breakdown." Mit Sloan Management Review **46**(1): 53-+.

Closs, D. J., M. A. Jacobs, M. Swink and G. S. Webb (2008). "Toward a theory of competencies for the management of product complexity: Six case studies." Journal of Operations Management **26**(5): 590-610.

Closs, D. J. and E. F. McGarral (2004). "Enhancing Security throughout the Supply Chain." IBM Centre for the Business of Government.

Cozzella, L., C. Simonetti and G. Schirripa Spagnolo (2012). "Drug packaging security by means of white-light speckle." Optics and Lasers in Engineering **50**(10): 1359-1371.

Crainic, T. G., K. H. Kim, B. Cynthia and L. Gilbert (2007). Chapter 8 Intermodal Transportation. Handbooks in Operations Research and Management Science, Elsevier. **Volume 14:** 467-537.

Croom, S., P. Romano and M. Giannakis (2000). "Supply chain management: an analytical framework for critical literature review." European Journal of Purchasing & Supply Management **6**(1): 67-83.

Crutch, M. (2006). The Benefits of Investing in Global Supply Chain Security: Executive Summary from the CVCR 2006 Roundtable Meeting. I. C. a. S. C. S. IBM, Lehigh University Center for Value Chain Research.

Cullinane, K. and N. Toy (2000). "Identifying influential attributes in freight route/mode choice decisions: a content analysis." Transportation Research Part E: Logistics and Transportation Review **36**(1): 41-53.

CUTR (2000). Analysis of Freight Movement Mode Choice Factors, The Center for Urban Transportation Research at the University of South Florida.

Danielis, R., E. Marcucci and L. Rotaris (2005). "Logistics managers' stated preferences for freight service attributes." Transportation Research Part E: Logistics and Transportation Review **41**(3): 201-215.

DG-TREN (2008). EU energy and transport in figures: @Statistical pocketbook 2007/2008.

DNV Consulting (2005). Study on the impacts of possible European legislation to improve transport security. Report 3: Securing the Supply Chain, European Commission DG TREN.

DNV Consulting (2005). Study on the impacts of possible European legislation to improve transport security. Report 4: Securing the Infrastructure, European Commission DG TREN.

Drucker, P. F. (1973). "The Performance Gap in Management Science: Reasons and Remedies." Organizational Dynamics **2**(2): 19-29.

Dulbecco, P. and B. Laporte (2005). "How can the security of international trade be financed in developing countries? A global public good Approach." World Development **33**(8): 1201-1214.

Dullaert, W., B. Vernimmen, E.-h. Aghezzaf and B. Raa (2007). Revisiting Service-level Measurement for an Inventory System with Different Transport Modes. Transport Reviews, Routledge. **27:** 273-283.

EC (2006). COMMUNICATION on Enhancing Supply Chain Security. Brussels, Commission of the European Communities.

EC (2006). ZWB Pilotbericht. E. T. a. C. Union. Brussels, CSP Customs and Services Programme.

EC (2008). Greening Transport. Brussels, Commission of the European Communities.

ECMT (2001). Terminology on Combined Transport. New York and Geneva, United Nations.

Enyinda, C. I. and D. Tolliver (2009). "Taking Counterfeits out of the Pharmaceutical Supply Chain in Nigeria: Leveraging Multilayer Mitigation Approach." Journal of African Business **10**(2): 218-234.

Erkut, E. and A. Ingolfsson (2000). "Catastrophe avoidance models for hazardous materials route planning." Transportation Science **34**(2): 165-179.

Esper, T. L. and L. R. Williams (2003). "The value of Collaborative Transportation Management (CTM): Its relationship to CPFR and information technology." Transportation Journal **42**(4): 55-65.

EU. (2006). "EU takes anti-terrorism fight to road and rail haulage." Retrieved September 7, 2006, from http://www.euractiv.com/en/transport/eu-takes-anti-terrorism-fight-road-rail-haulage/article-153022.

European Commission (2009). A sustainable future for transport. Towards an integrated, technology-led and user-friendly system.

European Shippers Council (2004). The Impact of Security Regulation and other Requirements on Shippers. OECD Workshop on Maritime Transport. Paris, OECD.

Eurostat (2009). Modal Split of Freight Transport, Statistical Office of the European Communities

Fischer, S. (2005). "Sicherheit in der Logistik: Mafiose Machenschaften." Logistik Heute **27**(3): 52-54.

Fletcher, T. (2007). "Authorized Economic Operator (AEO) Programs: IBM's Perspective." World Customs Journal **1**(2): 61-65.

Francis, V. (2008). "Supply chain visibility: lost in translation?" Supply Chain Management: An International Journal **13**(3): 180 - 184.

Füngerlings, F. (2001). Verbesserung des Sicherheitsniveaus der Binnen-Fahrgastschiffe in Europa PhDThesis, Bergische Universität - Gesamthochschule Wuppertal.

Gould, J. (2007). "Supply Chain Security: An Overview of Theoretical Applications." LogDynamics Research Report **1**.

Gould, J. E. (2010). A Decision Support System for Intermodal Logistics under Considerations for Cost and Security. Bremen, Universität Bremen. **Dissertation**.

Grainger, A. (2007). "Supply Chain Security: Adding to a Complex Operational and Institutional Environment." World Customs Journal **Vol 1**(Issue 2).

Gutiérrez, X., J. Hintsa, P. Wieser and A.-P. Hameri (2007). "Voluntary Supply Chain Security Program Impacts: An Empirical Study with BASC Member Companies." World Customs Journal **Volume 1**(Issue 2).

Haag, J. (2007). "Explosionsfeste Transportbehälter: Mehr Sicherheit für das Transportwesen." Packreport **40**(3): 52-54.

Haasis, H.-D. (2008). Produktions- und Logistikmanagement : Planung und Gestaltung von Wertschöpfungsprozessen. Wiesbaden, Gabler.

Hale, T. and C. R. Moberg (2005). "Improving supply chain disaster preparedness: A decision process for secure site location." International Journal of Physical Distribution & Logistics Management **35**(3): 195 - 207.

Hameri, A.-P. and J. Hintsa (2009). "Assessing the drivers of change for cross-border supply chains." International Journal of Physical Distribution & Logistics Management **39**(9): 741 - 761.

Hauge, J. B., V. Boschian and P. Pagenelli (2009). Synchronisation of material and information flows in intermodal freight transport- an industrial case study. Dynamics in Logistics, Second International Conference, LDIC 2009, Preproceedings. Bremen, Germany, August 17 - 21, 2009.

Hendricks, K. B. and V. R. Singhal (2003). "The effect of supply chain glitches on shareholder wealth." Journal of Operations Management **21**(5): 501-522.

Hesse, M. and J.-P. Rodrigue (2004). "The transport geography of logistics and freight distribution." Journal of Transport Geography **12**(3): 171-184.

Hiles, A. and P. Barnes, Eds. (2001). The Definitive Handbook of Business Continuity Management, John Wiley & Sons, Ltd.

Hintsa, J. (2010). "A comprehensive framework for analysis and design of supply chain security standards." Journal of Transportation Security.

Hintsa, J., X. Gutierrez, P. Wieser and A.-P. Hameri (2009). "Supply Chain Security Management: an overview." International Journal of Logistics Systems and Management **5**(3): 344-355.

Huang, G. Q., X. Y. Zhang and L. Liang (2005). "Towards integrated optimal configuration of platform products, manufacturing processes, and supply chains." Journal of Operations Management **23**(3-4): 267-290.

Ihde, G. (2001). Transport, Verkehr, Logistik: gesamtwirtschaftliche Aspekte und einzelwirtschaftliche Handhabung. München, Vahlen.

Institut für Mobilitätsforschung (2007). Qualitative Aspects of Transport Infrastructure. Transport, Trade and Economic Growth — Coupled or Decoupled? Institut für Mobilitätsforschung. Berlin, Springer**:** pp. 77-106.

Institut für Mobilitätsforschung, Ed. (2007). Transport, Trade and Economic Growth - Coupled or Decoupled? An Inquiry into Relationships between Transport, Trade and Economic Growth and into User Preferences concerning Growth-oriented Transport Policy. Mobilitätsverhalten in der Freizeit Springer Berlin Heidelberg.

INTEGRITY and SMART-CM (2008). Global Container Supply Chain Compendium.

ISL (2006). Comparitive Benchmarking of Performance for Freight Transport Across Modes from the Perspective of Transport Users: SSS vis-à-vis Rail, Road and IW. MTCP Study, Sixth Framework Programme, DG TREN, ISL Project Number 2341. Bremen, Germany, ISL Institute of Shipping Economics and Logistics.

ISO (2007). ISO 28000 2007 Specification for Security Management Systems for the Supply Chain. Geneva, Switzerland, International Organization for Standardization.

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

Kempf, J. (2008). Innovative Loesungen zur Verlustreduzierung in der Supply Chain. Sicherheit und Risikomanagement in der Supply Chain: Gestaltungsansaetze und praktische Umsetzung. H.-C. Pfohl. Hamburg, Bundesvereinigung Logistik, DVV-Media-Group, Dt. Verkehrs-Verl.**:** 333-341.

Kern, E.-M. (2007). "Management von Sicherheit in Supply Chains Möglichkeiten und Grenzen der Zertifizierung?" Industrie Management **23**(5): 63-66.

Kerschbaum, F., A. Schröpfer, A. Zilli, R. Pibernik, O. Catrina, S. d. Hoogh, B. Schoenmakers, S. Cimato and E. Damiani (2011). "Secure collaborative supply-chain management." Computer **44**(9): 38 - 43.

Ketchen, J. D. J. and G. T. M. Hult (2007). "Bridging organization theory and supply chain management: The case of best value supply chains." Journal of Operations Management **25**(2): 573-580.

Knemeyer, A. M., W. Zinn and C. Eroglu (2008). "Proactive planning for catastrophic events in supply chains." Journal of Operations Management **In Press, Corrected Proof**.

Koopmans, T. C. (1951). "Efficient Allocation of Resources." Econometrica **19**(4): 455-465.

Kotsiwos, A. (2008). Transport-Sicherheit in der Logistik - auch ein globales Thema. Global Logistics: Strategien - Konzepte - Praxisbeispiele. F. Straube, T. Beckmann, M. Bdhn, J. Fontius and A. Wieland, Bundesvereinigung Logistik, DVV-Media-Group, Dt. Verkehrs-Verl.**:** 167-179.

Kumar, S., H. Jensen and H. Menge (2008). "Analyzing Mitigation of Container Security Risks Using Six Sigma DMAIC Approach in Supply Chain Design." Transportation Journal **47**(2): 54-66.

Kumar, S. and J. Verruso (2008). "Risk Assessment for the Security of Inbound Containers at U.S. Ports: A Failure, Mode, Effects, and Criticality Analysis Approach." Transportation Journal **47**(4): 26-41.

Laeequddin, M., G. D. Sardana, B. S. Sahay, K. A. Waheed and V. Sahay (2009). "Supply chain partners' trust building process through risk evaluation: the perspectives of UAE packaged food industry." Supply Chain Management: An International Journal **14**(4): 280 - 290.

Lake, J. E., W. H. Robinson and L. M. Seghetti (2005). Border and Transportation Security: The Complexity of the Challenge, Congressional Research Service RL32839 March 29, 2005.

Lee, H. L. (2004). Supply Chain Security: Are You Ready? Stanford, CA, Stanford Global Supply Chain Management Forum.

Lee, H. L. and S. Whang (2003). Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management, Stanford University, Graduate School of Business, Research Papers.

Lindroth, R. and A. Norrman (2001). Supply Chain Risk and Risk Sharing Instruments - An Illustration from the Telecommunication Industry. Proceedings of the Logistics Research Network 6th Annual Conference, September 13-14, 2001. L. R. Network. Heriot-Watt University, Institute of Logistics and Transport**:** 297-307.

Lintukangas, K., S. Peltola and V.-M. Virolainen (2009). "Some issues of supply management integration." Journal of Purchasing and Supply Management **15**(4): 240-248.

Little, J. D. C. (1970). "Models and Managers: The Concept of a Decision Calculus." Management Science **16**(8): B466-B485.

Logistik Heute (2005). Sicherheit in der Logistik: Alles im Blick. **27:** 60-61.

Logistik Heute (2008). Wettbewerbsvorteil: Sicherheit. Logistik Heute. **12:** 64-65.

Lu, C.-S. and C.-C. Yang (2007). "An evaluation of the investment environment in international logistics zones: A Taiwanese manufacturer's perspective." International Journal of Production Economics **107**(1): 279-300.

Luedtke, J. and C. C. White, III (2002). HAZMAT Transportation and Security: Survey and Directions for Future Research. Atlanta, Georgia, Department of Industrial and Systems Engineering Georgia Institute of Technology.

Macharis, C. and Y. M. Bontekoning (2004). "Opportunities for OR in intermodal freight transport research: A review." European Journal of Operational Research **153**(2): 400-416.

Macharis, C., E. Pekin, A. Caris and B. Jourquin (2008). A Decision Support System for Intermodal Transport Policy Brussels, VUBPress.

Macharis, C., E. Van Hoeck, E. Pekin and T. van Lier (2010). "A decision analysis framework for intermodal transport: Comparing fuel price increases and the internalisation of external costs." Transportation Research Part A: Policy and Practice **44**(7): 550-561.

Macharis, C., K. Van Raemdonck, J. Hintsa and O. Mairesse (2012). Multimodal Analysis Framework for Hazmat Transports and Security. Security Aspects of Uni- and Multimodal Hazmat Transportation Systems, Wiley-VCH Verlag GmbH & Co. KGaA**:** 135-162.

Macpherson, A. D. and J. E. McConnell (2007). "A Survey of Cross-Border Trade at a Time of Heightened Security: The Case of the Niagara Bi-National Region." American Review of Canadian Studies **37**(3): 301 - 321.

Manuj, I. and J. T. Mentzer (2008). "Global supply chain risk management strategies." International Journal of Physical Distribution & Logistics Management **38**(3): 192 - 223.

Marasco, A. (2008). "Third-party logistics: A literature review." International Journal of Production Economics **113**(1): 127-147.

Martha, J. and S. Subbakrishna (2002). "Targeting a just-in-case supply chain for the inevitable next disaster? ." Supply Chain Management Review **September/October**: 18-23.

McGinnis, M. A. (1989). "A Comparative Evaluation of Freight Transportation Choice Models." Transportation Journal **29**(2): 36-46.

Meixell, M. J. and M. Norbis (2008). "A review of the transportation mode choice and carrier selection literature." The International Journal of Logistics Management **19**(2): 183 - 211.

Mentzer, J. T. (1991). "AN EFFICIENCY/EFFECTIVENESS APPROACH TO LOGISTICS PERFORMANCE ANALYSIS." Journal of Business Logistics **12**(1): 33-62.

Mentzer, J. T., W. DeWitt, J. S. Keebler, M. Soonhoong, N. W. Nix, C. D. Smith and Z. G. Zacharia (2001). "DEFINING SUPPLY CHAIN MANAGEMENT." Journal of Business Logistics **22**(2): 1-25.

Mikuriya, K. (2007). "Supply Chain Security: the Customs Community's Response." World Customs Journal **1**(2): 51-59.

Müller, R. (2008). Developing a Security Event Management System for Intermodal Transport. Dynamics in Logistics. H.-J. Kreowski, B. Scholz-Reiter and H.-D. Haasis, Springer Berlin Heidelberg**:** 405-412.

Neumann, T. (2008). Prozesssicherheit entlang der Supply Chain. Sicherheit und Risikomanagement in der Supply Chain: Gestaltungsansaetze und praktische Umsetzung. H.-C. Pfohl. Hamburg, Bundesvereinigung Logistik, DVV-Media-Group, Dt. Verkehrs-Verl.**:** 319-332.

Nevrous, K. (2010). "Secure supply chain management in a changing world of threats." Deloitte Service LP, Deloitte Risk Services.

New, S. J. (1997). "The scope of supply chain management research." Supply Chain Management: An International Journal **2**(1): 15 - 22.

New, S. J. and P. Payne (1995). "Research frameworks in logistics: three models, seven dinners and a survey." International Journal of Physical Distribution & Logistics Management **25**(10): 60 - 77.

Norrman, A. and U. Jansson (2004). "Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident." International Journal of Physical Distribution & Logistics Management **34**(5): 434 - 456.

Notteboom, T. E. and J.-P. Rodrigue (2005). "Port regionalization: towards a new phase in port development." Maritime Policy & Management: The flagship journal of international shipping and port research **32**(3): 297 - 313.

OECD (2003). Security in Maritime Transport: Risk Factors and Economic Impact. Paris, Maritime Transport Committee, Organization for Economic Cooperation and Development.

OECD (2005). Container transport security across modes. Paris, OECD.

Peck, H. (2005). "Drivers of supply chain vulnerability: an integrated framework." International Journal of Physical Distribution & Logistics Management **35**(4): 210-232.

Peck, H. (2006). "Reconciling supply chain vulnerability, risk and supply chain management." International Journal of Logistics: Research and Applications **Vol. 9**((2)): pp.127-142.

Peleg-Gillai, B., G. Bhat and L. Sept (2006). Innovators in Supply Chain Security: Better Security Drives Business Value. The Manufacturing Innovation Series. T. M. Institute, Standford University.

Plöger, M. and H.-D. Haasis (2009). Overcoming information integration barriers in multi-tier supply chains with programmable RFID devices, Institute of Shipping Economics and Logistics (ISL).

Prato, C. G. (2009). "Route choice modeling: past, present and future research directions." Journal of Choice Modelling **2**(1): 51-64.

Rice, J. B., Jr., (2007). "Rethinking Security." Logistics Management **May 2007**.

Romero, C. (1991). Handbook of Critical Issues in Goal Programming. Oxford, Pergamon Press.

Sanchez, R. and A. Heene (2004). The new strategic management : organization, competition and competence. New York ; [London], Wiley.

Saxton, J. (2002). The Economic Costs of Terrorism. J. E. Committee. Washington, D.C., United States Congress.

Schönberger, J. and H. Kopfer (2009). "Online decision making and automatic decision model adaptation." Computers & Operations Research **36**(6): 1740-1750.

Sheffi, Y. (1985). "Some analytical problems in logistics research." Transportation Research Part A: General **19**(5-6): 402-405.

Sheffi, Y. (2001). "Supply Chain Management under the Threat of International Terrorism." International Journal of Logistics Management **12**: 1-11.

Sherali, H. D., L. D. Brizendine, T. S. Glickman and S. Subramanian (1997). "Low-Probability-High Consequence Considerations in Routing Hazardous Material Shipments." Transportation Science **31**(3): 237.

Sheu, C., L. Lee and B. Niehoff (2006). "A voluntary logistics security program and international supply chain partnership." Supply Chain Management: An International Journal **11**(4): 363 - 374.

Sroufe, R. and S. Curkovic (2008). "An examination of ISO 9000:2000 and supply chain quality assurance." Journal of Operations Management **26**(4): 503-520.

Stadtler, H., Ed. (2008). Supply Chain Management and Advanced Planning, Springer Berlin Heidelberg.

Stock, G. N., N. P. Greis and J. D. Kasarda (2000). "Enterprise logistics and supply chain structure: the role of fit." Journal of Operations Management **18**(5): 531-547.

Stonebraker, P. W. and R. Afifi (2004). "Toward a contingency theory of supply chains." Management Decision **42**(9): 1131 - 1144.

Svensson, G. (2003). "Holistic and cross-disciplinary deficiencies in the theory generation of supply chain management." Supply Chain Management-an International Journal **8**(3-4): 303-316.

Svensson, G. (2004). "Key areas, causes and contingency planning of corporate vulnerability in supply chains: A qualitative approach." International Journal of Physical Distribution & Logistics Management **34**(9): 728-748.

Tan, K. C. (2001). "A framework of supply chain management literature." European Journal of Purchasing & Supply Management **7**(1): 39-48.

Tavasszy, L. A., C. J. Ruijgrok and M. J. P. M. Thissen (2003). "Emerging Global Logistics Networks: Implications for Transport Systems and Policies." Growth & Change **34**(4): 456-472.

Thai, V. V. (2009). "Effective maritime security: conceptual model and empirical evidence." Maritime Policy & Management **36**(2): 147-163.

Thomas, A. (2008). "Editor's note: The case for a transportation security research agenda." Journal of Transportation Security **1**(1): 1-2.

Timmerman, P. (1981). Vulnerability, resilience and the collapse of society : A review of models and possible climatic applications. Toronto, Canada, University of Toronto.

Transportation Research Board (2002). Deterrence, protection, and preparation : the new transportation security imperative. Special report. Washington, D.C., Transportation Research Board**:** x, 84 p.

Tzannatos, E. S. (2003). "A decision support system for the promotion of security in shipping." Disaster Prevention and Management **12**(3): 222-229.

USCBP (2006). Container Security Initiative: 2006-2011 Strategic Plan. Office of Policy and Planning and Office of International Affairs Container Security Initiative Division. Washington, D.C.

USCBP. (2008, March 20, 2010). "Container Security Initiative in Brief." Retrieved April 24, 2010, from http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/csi_in_brief.xml.

USCBP. (2009). "Customs-Trade Partnership Against Terrorism: 2008 - A Year in Review." Retrieved April 24, 2010, from http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/what_ctpat/2008_year_review.ctt/2008_year_review.pdf.

USCBP. (2009). "Customs-Trade Partnership Against Terrorism: A Guide to Benefits." Retrieved April 24, 2010, from http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_benefits.ctt/ctpat_benefits.pdf.

Ustundag, A. and M. Tanyas (2009). "The impacts of Radio Frequency Identification (RFID) technology on supply chain costs." Transportation Research Part E: Logistics and Transportation Review **45**(1): 29-38.

van Duin, R. and H. van Ham (1998). A three-stage modeling approach for the design and organization of intermodal transportation services. Systems, Man, and Cybernetics, 1998. 1998 IEEE International Conference on.

Vance, A. (2008). "Strategic Responses by Canadian and U.S. Exporters to Increased U.S. Border Security Measures: A Firm-Level Analysis." Economic Development Quarterly **22**(3): 239-251.

Vannieuwenhuyse, B., L. Gelders and L. Pintelon (2003). "An online decision support system for transportation mode choice." Logistics Information Management **16**(2): 125-133.

Varkonyi, I. (2004). "Breaking down silos in supply-chain security." Journal of Commerce (15307557) **5**(31): 53-53.

Vernimmen, B., W. Dullaert, P. Willemé and F. Witlox (2008). "Using the inventory-theoretic framework to determine cost-minimizing supply strategies in a stochastic setting." International Journal of Production Economics **115**(1): 248-259.

Voss, M. D., D. J. Closs, R. J. Calantone, O. K. Helferich and C. Speier (2009). The Role of Security in the Food Supplier Selection Decision. Journal of Business Logistics, Council of Supply Chain Management Professionals. **30:** 127-155.

Voss, M. D., J. M. Whipple and D. J. Closs (2009). "The Role of Strategic Security: Internal and External Security Measures with Security Performance Implications." Transportation Journal **48**(2): 5-23.

Wagner, S. M. and C. Bode (2006). "An empirical investigation into supply chain vulnerability." Journal of Purchasing and Supply Management **12**(6): 301-312.

Weise, H. (2005). "Sicherheit in der Logistik: Leichtes Spiel für Langfinger." Logistik Heute **27**(3): 56-57.

Whipple, J. M., M. D. Voss and D. J. Closs (2009). "Supply chain security practices in the food industry: Do firms operating globally and domestically differ?" International Journal of Physical Distribution & Logistics Management **39**(7): 574 - 594.

Whiting, M. C. and B. E. Ayala-Ostrom (2009). "Advocacy to promote logistics in humanitarian aid." Management Research News **32**(11): 1081 - 1089.

Wieland, A. (2008). Sicherheit in globalen Supply Chains. Global Logistics: Strategien - Konzepte - Praxisbeispiele. F. Straube, T. Beckmann, M. Bdhn, J. Fontius and A. Wieland, Bundesvereinigung Logistik, DVV-Media-Group, Dt. Verkehrs-Verl.**:** 143-151.

Williams, Z., J. E. Lueg and S. A. LeMay (2008). "Supply chain security: an overview and research agenda." The International Journal of Logistics Management **19**(2): 254 - 281.

Williams, Z., J. E. Lueg, R. D. Taylor and R. L. Cook (2009). "Why all the changes?: An institutional theory approach to exploring the drivers of supply chain security (SCS)." International Journal of Physical Distribution & Logistics Management **39**(7): 595 - 618.

Williams, Z., N. Ponder and C. W. Autry (2009). "Supply chain security culture: measure development and validation." The International Journal of Logistics Management **20**(2): 243 - 260.

Willis, H. H. and D. S. Oritz (2004). Evaluating the Security of the Global Containerized Supply Chain. RAND Corporation. Santa Monica, CA.

Wilson, M. C. (2007). "The impact of transportation disruptions on supply chain performance." Transportation Research Part E: Logistics and Transportation Review **43**(4): 295-320.

Witlox, F. (2003). Quality attributes in freight transport modelling. A literature review. Across the Border: Building Upon a Quarter Century of Transport Research in the Benelux. W. Dullaert, B. A. M. Jourquin and J. B. Polak. Antwerp, Uitgeverij De Boeck**:** pp. 27-41.

Witlox, F. and E. Vandaele (2005). "Determining the monetary value of quality attributes in freight transportation using a stated preference approach." Transportation Planning and Technology **28**(2): 77-92.

Wolfe, M. (2004). "The Dynamics of Supply Chain Security." The Monitor **10**(2).

World BASC Organization. (2005). "BASC - Business Alliance for Secure Commerce." Retrieved May 01, 2010, from http://www.wbasco.org/index-eng.htm.

World Customs Organization (2007). "WCO SAFE Framework of Standards."

World Customs Organization. (2012). "Compendium of Authorized Economic Operator Programmes." 2012. Retrieved August 2012, from http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Procedures%20and%20Facilitation/safe_package/AEO_Compendium_2012_en.pdf.

World Shipping Council. (2002). "Liner Shipping: Facts and Figures." Retrieved Last accessed on 31.09.2006, from http://www.worldshipping.org/liner_shipping-facts&figures.pdf.

Woxenius, J. (1999). A scenario for future European intermodalism. VTI's and KFB's Transport Forum. Linköping, 13-14 January

Yang, Y.-C. (2011). "Risk management of Taiwan's maritime supply chain security." Safety Science **49**(3): 382-393.

Zeleny, M. (1982). Multiple Criteria Decision Making. New York., McGraw-Hill.

Appendix GAMS Model of the Goal Programme

```
VARIABLES
      varZ                'Total Costs'


POSITIVE VARIABLES
      varAT(c,i)          'arrival time of consignment c at location i'

      varBTT(c,i,j,k)      'Transit Buffer time between location i and location j'

      varBTL(c,i)          'Buffer time at location i going to location j'


      varD_1_plus(c)       'Freight Costs'

      varD_2_plus(c)       'delay of consignments'

      varD_2_minus(c)       'early delivery of an consignment'

      varD_3_plus(c)       'loss, theft and damage of goods'

;


BINARY VARIABLE
      varbinX(c,i,j,k)     '1 if mode k between i and j is used. Otherwise 0'

;


EQUATIONS
      eq_01_ObjectiveFunction             'Min total costs C'

      eq_02_cost_goal(c)                  'Costs of transportation'

      eq_03_DeliveryDelay(c,i)            'TimeWindow'

      eq_04_NoEarlyDeliveries(c,i)        'TimeWindow'

      eq_05_InitialFlow(c,i)              'Flow Constraint'

      eq_06_BalanceFlow(c,d)              'Flow Constraint'
```

```
        eq_07_EndingFlow(c,i)               'Flow Constraint'
        eq_08_ArrivalTime_1(c,i,j)          'ArrivalTime at location d'
        eq_09_ArrivalTime_2(c,i,j)          'Arrival time at the first location after the origin'
        eq_10_ModeAssignment(c,i,j)         'Assignment of Modes'
        eq_11_Capacity(c,i,j,k)             'Capacity constraint'
        eq_12_ArrivalTime_3(c,i)            'Set all non used arrival times to zero'
        eq_13_BTT(c,i,j,k)                  'Set all non used transit buffer times to zero'
        eq_14_BTL(c,i)                      'Set all non used buffer times at locations to zero'
        eq_15_TimeBuffer(c,i,j)             'Computation of time buffer for transit without
origin'
        eq_16_TimeBuffer(c,i,j)             'Computation of time buffer for transit from the
origin'
        eq_17_LDRISK(c)                     'Computation of expected losses for transit time
buffers'
;


eq_01_objectivefunction..
        varZ =e=
            parW1*sum(c, varD_1_plus(c))
            + parW2*((sum(c, varD_2_plus(c))) + (sum(c, varD_2_minus(c))))
            + parW3*(sum(c, varD_3_plus(c)))
;


eq_02_cost_goal(c)..
        varD_1_plus(c) =e=
             sum(i, sum(j, sum(k$ijk(i, j, k), parFR(i,j,k)*parS(c)*varbinX(c,i,j,k))))
```

```
;

eq_03_DeliveryDelay(c,i)$cd(c,i)..
        varAT(c,i)-parDT(c) - varD_2_plus(c) + varD_2_minus(c) =e= 0
;

eq_04_NoEarlyDeliveries(c,i)$cd(c,i)..
        parET(c) =l=
                varAT(c,i)
;

eq_05_InitialFlow(c,i)$co(c, i)..
        sum( j, sum(k$ijk(i, j, k), varbinX(c,i,j,k))) =e= 1
;

eq_06_BalanceFlow(c,d)$((NOT co(c, d)) AND (NOT cd(c, d)))..
       sum(i, sum(k$ijk(i, d, k), varbinX(c,i,d,k))) =e=
              sum(j, sum(k$ijk(d, j, k), varbinX(c,d,j,k)))
;

eq_07_EndingFlow(c,j)$cd(c, j)..
        sum( i, sum(k$ijk(i, j, k), varbinX(c,i,j,k))) =e= 1
;

eq_08_ArrivalTime_1(c,i,j)$((ij(i, j))AND (NOT co(c, j)))..
```

```
        varAT(c,i)
        + sum(k$ijk(i, j, k), varbinX(c,i,j,k)*(parLDT(k)+parTT(i,j,k)+parUDT(k))) =l=
              varAT(c,j)
              + (2
                    -sum(d, sum(k$ijk(d, i, k), varbinX(c,d,i,k)))
                    -sum(l$ijk(i, j, l), varbinX(c,i,j,l)))*parBigM

;

eq_09_ArrivalTime_2(c,i,j)$((ij(i, j))AND (NOT co(c, j)) AND (co(c, i)))..
        varAT(c,i)
       + parIT(c)
        + sum(k$ijk(i, j, k), varbinX(c,i,j,k)*(parLDT(k)+parTT(i,j,k)+parUDT(k))) =l=
              varAT(c,j)
              + (1
                    -sum(l$ijk(i, j, l), varbinX(c,i,j,l)))*parBigM
;

eq_10_ModeAssignment(c,i,j)..
        sum(k$ijk(i, j, k), varbinX(c,i,j,k)) =l= 1
;

eq_11_Capacity(c,i,j,k)$ijk(i, j, k)..
        parS(c)*varbinX(c,i,j,k) =L= parCap(i,j,k)
;
```

```
eq_12_ArrivalTime_3(c,i)..
        varAT(c,i) =l=
              sum(j, sum(k$ijk(j, i, k), varbinX(c,j,i,k)))*parBigM
;


eq_13_BTT(c,i,j,k)$ijk(i, j, k)..
        varBTT(c,i,j,k) =l=
               varbinX(c,i,j,k)*parBigM
;


eq_14_BTL(c,i)..
        varBTL(c,i) =l=
               sum(j, sum(k$ijk(i, j, k), varbinX(c,i,j,k)))*parBigM
;


eq_15_TimeBuffer(c,i,j)$((ij(i, j))AND (NOT co(c, j)))..
        varAT(c,j)
        - varAT(c,i)
        - sum(k$ijk(i, j, k), varbinX(c,i,j,k)*(parLDT(k)+parTT(i,j,k)+parUDT(k)))
        - varBTL(c,i) =l=
              sum(k$ijk(i, j, k), varBTT(c,i,j,k))
              + (2
                    -sum(d, sum(k$ijk(d, i, k), varbinX(c,d,i,k)))
                    -sum(l$ijk(i, j, l), varbinX(c,i,j,l)))*parBigM
```

```
;

eq_16_TimeBuffer(c,i,j)$((ij(i, j))AND (NOT co(c, j)) AND (co(c, i))).. 
        varAT(c,j)
        - varAT(c,i)
        - parIT(c)
        - varBTL(c,i)
        - sum(k$ijk(i, j, k), varbinX(c,i,j,k)*(parLDT(k)+parTT(i,j,k)+parUDT(k))) =l=
              sum(k$ijk(i, j, k), varBTT(c,i,j,k))
              + (1
                    -sum(l$ijk(i, j, l), varbinX(c,i,j,l)))*parBigM
;

eq_17_LDRISK(c)..
        sum(i, sum(j, sum(k$ijk(i, j, k), varbinX(c,i,j,k)*parLD(i,j,k)*parS(c)))) +
        sum(i, sum(j, sum(k$ijk(i, j, k), varBTT(c,i,j,k)*parPen(i,j,k)*parSR(c)*parS(c)))) +
        sum(i, varBTL(c,i)*parPenN(i)*parSR(c)*parS(c)) - varD_3_plus(c) =e= 0
;


MODEL GP /all/;


OPTION optcr = 0.001;
*Test.reslim = 600;
```

```
*Test.OptFile =1;

*OPTION minlp = baron;


SOLVE GP using MIP minimizing varZ;
```