Managing the Risk for Antagonistic Threats against the Transport Network

DANIEL EKWALL

Department of Technology Management and Economics
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2009

School of Engineering
UNIVERSITY OF BORÅS
Borås, Sweden 2009
Managing the Risk for Antagonistic Threats against the Transport Network

ISBN 978-91-7385-249-4

© Daniel Ekwall, 2009

Doktorsavhandlingar vid Chalmers tekniska högskola:
Ny serie nr 2930
ISSN 0346-718X
This electronic edition contains minor revisions to the printed version, mainly regarding spelling and typographic errors. The printed version has been supplemented with an errata-list containing these changes.

Department of Technology Management and Economics
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31 – 772 1000

Printed by Chalmers Reproservice
Göteborg, Sweden 2007

Skrifter från Högskolan i Borås: 15
ISSN 0280-381X

School of Engineering
University of Borås
SE-501 90 Borås, Sweden
Managing the Risk for Antagonistic Threats against the Transport Network

Daniel Ekwall

Department of Technology Management and Economics
Chalmers University of Technology

Abstract

The World Trade Centre terror attack in 2001 changed the world and with it the conditions for logistics worldwide. The aftermath of the attack brought needed attention to the vulnerability of modern supply chains. This thesis addresses the antagonistic threats that exploit the vulnerability in a supply chain. Antagonistic threats are a limited array of risks and uncertainties and can be addressed with risk management tools and strategies. There are three key demarcations between antagonistic threats and other risks and uncertainties: deliberate (caused), illegal (defined by law), and hostile (negative impact, in this thesis, for transport network activities). This thesis makes a theoretical contribution to the usage of theories from criminology in supply chain risk management to handle antagonistic threats against the transport network. The recognition that antagonistic threats toward the transport network are a problem leads to verification of the research questions from the background and the theoretical framework. This is done to place or relate the research questions closer to the context. Furthermore, it leads to the conclusion that the answers may or may not contain competing and/or incompatible parts which differ depending on the perspective or viewpoint at the moment. One of the most important things to understand is that antagonistic threats toward freight always have been a feature in both business and politics. The different functions and goals for all stakeholders mean that all stakeholders and actors may use similar methods to manage antagonistic threats but the effects and consequences will change according to the circumstances.

The system approach in this thesis is a soft-system thinking where reality is described in subjective terms and the whole system has the distinctive trait of vague or undefined boundaries between system components and the surrounding environment. Therefore, this thesis uses a complex system approach in which paradoxes and bounded rationality describes the system’s behaviour. This thesis defines the legal descriptions and criminal threats against and within supply chain management activities that entail both the systems context and boundaries. Managing of the antagonistic threats through the risk management perspective is separated into two sides, pre-event and post-event measures, which means the system needs to be robust and resilient, using logistics terms. It should be robust to automatically handle small risks (normally with high likelihood and low impact). The system also needs resilience in order to adapt, improvise, and overcome any disturbance greater than the system’s robustness can handle. Both robustness and its resilience can constitute of the full range of prevention, mitigation, and transferring tools and methods. Regardless of which perspective or viewpoint is chosen for analysing the problem, the same basic set of tools and methods are valid, but in practical use they need to be adapted to the actors’ needs and wants for managing their exposure to antagonistic threats.

Keywords: Supply chain management, transport network, risk management, crime prevention, supply chain risk management, Supply chain security
“The whole of science is nothing more than refinement of everyday thinking”
Albert Einstein

“Everything is different but nothing seems to have changed”
Friedrich Nietzsche

“Don't get involved in partial problems, but always take flight to where there is a free view over the whole single great problem, even if this view is still not a clear one.”
Ludwig Wittgenstein
Preface

This thesis has been written at the School of Engineering at the University of Borås. Although it is the result of my own effort, the thesis would not have been finished without the support and help from colleagues, family, and friends. Therefore, I would like to thank you all.

The financial support of this thesis comes from both the University of Borås and the Swedish Governmental Agency for Innovation Systems (VINNOVA). I would like to thank both organizations for their trust in me and my research. The results of this thesis depend on the cooperation of the companies and organizations that shared information, discussed theories, and the reality with me. Without their experience and knowledge the result would not have been the same.

I want to express my gratitude to my supervisors, Professor Håkan Torstensson, University of Borås, and Professor Kenth Lumsdén, Chalmers University of Technology. Without their support, advice, and trust, this thesis would never been completed. Professor Torstensson deserves recognition for his patience with the research process and my many wild research ideas, and Professor Lumsdén for the relaxed confidence he always has had in me. I wish to thank Bertil Rolandsson, Ph.D., University of Borås, for good discussion and collaboration with regard to theories and methods from criminology and social sciences. Thanks to Fredrik Nilsson, Ph.D., Lund University, for introducing me to complexity theory, the cement that holds this thesis together. I wish to thank Professor Stig Franzén, Chalmers University of Technology, for providing the vital comments on this thesis during the final stages of completion. A special thank you to Göran Berg, Swedish Transport Agency, for his practical knowledge of security and business politics.

During the research process, several other colleagues at the University of Borås, School of Engineering’s section for quality-driven logistics and the Swedish School of Textiles’ section for applied textile management have provided support and contributed to the outcome. Thank you all. I would also like to thank the helpful personnel at the library and learning resources department and the rest of the employees at the University of Borås. A special thanks to professors, colleagues, and other personnel at Chalmers University of Technology’s Division of Logistics and Transportation for their help during the research process. A final thanks to my colleagues at the Corporate Risk Management department at Schenker AG for their expertise in insurances and claims in a multinational logistics company.

My thanks to all my friends, who continued to be my friends, despite my never-ending talk about my research and absence from dinner parties. A special warm acknowledgment to my family for believing in me. Special thanks to my parents for their support through the years.

Last, but by no means least, thanks for the support I have received from my wife Lovisa. Without your understanding and encouragement, I never would have been able to finish this thesis. Finally, thanks to my son, Otto, for your existence. You have contributed more than you know. I love you both!

Borås, February 2009

Daniel Ekwall
List of appended papers

PAPER A:


Winner of DB Schenker’s Award for best for the best doctoral student paper at Nofoma 2008


PAPER B:


PAPER C:

Ekwall, D. and Lumsden, K. (2007), “Differences in stakeholder opinion regarding antagonistic gateways within the transport network”. In proceedings of Nofoma, Rejkavik

PAPER D:


PAPER E:


Submitted to Nofoma 2009, Jönköping

PAPER F:


PAPER G:


PAPER H:

Mazeradi, A. and Ekwall, D. (2009), ”Impacts of the ISPS code on port activities – A case study on Swedish ports”.

Accepted for publication (Vol. 2, No 4, 2009) in World Review of Intermodal Transportation Research special issue on “Northern dimension of European logistics”
# Table of content

List of figures XI  
List of tables XII  

1. **Introduction**  
   1.1. *Background*  
      1.1.1. Definition of antagonistic threats  
      1.1.2. Antagonistic threats against the transport network  
      1.1.3. Theft of cargo, vehicles, and driver belonging  
      1.1.4. Smuggling of goods  
      1.1.5. Terrorism threats  
      1.1.6. Shrinkage or loss for different actors in a supply chain  
      1.1.7. Insurance claims (FFL) for one of the worlds leading LSP  
      1.1.8. Cargo theft in Europe  
      1.1.9. Cargo theft in Sweden  
   1.2. *Purpose*  
   1.3. *Scope*  
   1.4. *Limitations*  
   1.5. *Antagonistic threats as a wicked problem*  
   1.6. *Research questions*  
   1.7. *Outline of the thesis*  

2. **Frame of reference**  
   2.1. *Components in the framework*  
   2.2. *The supply chain concepts*  
       2.2.1. Principles of microeconomics as a business description  
       2.2.2. The market and the end user  
   2.3. *System of supply chains*  
   2.4. *Supply chain, logistics and transport*  
   2.5. *Risk and uncertainty in the supply chain*  
   2.6. *Supply chain vulnerability*  
   2.7. *Supply chain risk management*  
   2.8. *Supply chain security*  
   2.9. *Risk management and security in a supply chain context*  
       2.9.1. Transport and freight security  
       2.9.2. Logistics security programmes  
       2.9.3. System of supply chain risks  
   2.10. *The insurance principle; conventions, claims, and premiums*  
       2.10.1. The CMR convention  
       2.10.2. Enhanced liability in insurance  
       2.10.3. Incoterms 2000  
   2.11. *Criminology and logistics*  
       2.11.1. The two different outlooks on mankind in criminology  
       2.11.2. Criminal prosecution and punishment  
       2.11.3. Opportunity to crime  
       2.11.4. Routine activity perspective
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.</td>
<td>Generalisation</td>
<td>101</td>
</tr>
<tr>
<td>6.3.</td>
<td>Generalisation of managing the risk of antagonistic threats</td>
<td>102</td>
</tr>
<tr>
<td>6.3.1.</td>
<td>Perpetrator and threat opportunity</td>
<td>103</td>
</tr>
<tr>
<td>6.3.2.</td>
<td>Mitigation of antagonistic threats</td>
<td>103</td>
</tr>
<tr>
<td>6.3.3.</td>
<td>Transfer of antagonistic threats</td>
<td>104</td>
</tr>
<tr>
<td>6.3.4.</td>
<td>Compliance with logistics security programmes</td>
<td>104</td>
</tr>
<tr>
<td>6.3.5.</td>
<td>Cargo crime as a production method</td>
<td>105</td>
</tr>
<tr>
<td>6.3.6.</td>
<td>Terrorist threat toward logistics operations</td>
<td>106</td>
</tr>
<tr>
<td>7.</td>
<td>Conclusions and future research</td>
<td>108</td>
</tr>
<tr>
<td>7.1.</td>
<td>Conclusions</td>
<td>108</td>
</tr>
<tr>
<td>7.1.1.</td>
<td>Proportions and patterns of the problem</td>
<td>108</td>
</tr>
<tr>
<td>7.1.2.</td>
<td>Understanding of the problem</td>
<td>109</td>
</tr>
<tr>
<td>7.1.3.</td>
<td>Managing the problem</td>
<td>110</td>
</tr>
<tr>
<td>7.2.</td>
<td>Future research</td>
<td>111</td>
</tr>
<tr>
<td></td>
<td>General ideas for future research areas</td>
<td>111</td>
</tr>
<tr>
<td></td>
<td>Suggestion for future papers</td>
<td>112</td>
</tr>
<tr>
<td>8.</td>
<td>References</td>
<td>114</td>
</tr>
</tbody>
</table>

Appendix A - Additional publication by the author | 132  |
Appendix B - List of organizations involved during the research process | 134  |
Appendix C – Glossary and Abbreviations | 136  |
Appendix D – Cost calculation for cargo theft in Sweden | 138  |
| Figure 1: The produce/acquire matrix and legality of the business | 2 |
| Figure 2: Supply chain risk management — basic Constructs (Juttner et al., 2003) | 3 |
| Figure 3: Antagonist threats against the transport network | 5 |
| Figure 4: The relationship between the frame of reference and the research questions | 20 |
| Figure 5: Thesis outline | 23 |
| Figure 6: Presentation of the theoretical framework for this thesis | 24 |
| Figure 7: The dialectic relationship between logistics and transport (Arnäs, 2007; Sjöstedt, 2005) | 28 |
| Figure 8: The five needs for logistics fulfilment | 30 |
| Figure 9: Freight distribution and network strategies (Hesse et al., 2004) | 31 |
| Figure 10: The basic process of risk management (Waters, 2007) | 33 |
| Figure 11: Sources of supply chain risks (Christopher et al, 2004) | 34 |
| Figure 12: Vulnerability of the supply chain (Waters, 2007) | 35 |
| Figure 13: Constraints and disturbance risk affecting the five needs for logistics fulfilment | 36 |
| Figure 14: Cause/consequence matrix for cargo incidents | 40 |
| Figure 15: Security in the transport network | 42 |
| Figure 16: The division of risk from consignor to consignee by Incoterms 2000 | 48 |
| Figure 17: Perpetrator’s characteristics matrix | 56 |
| Figure 18: The antagonistic threat triangle in logistics | 59 |
| Figure 19: Research chronology | 67 |
| Figure 20: Links between appended papers and the thesis model | 73 |
| Figure 21: The antagonistic threat triangle | 92 |
| Figure 22: Supply chain risk management — basic Constructs (Juttner et al., 2003) | 97 |
| Figure 23: Antagonist threats against the transport network | 99 |
| Figure 24: General model for managing antagonistic threats | 102 |
| Figure 25: Costs comparison example between legal business and cargo crimes | 106 |
| Figure 26: Links between suggested future papers and this thesis model | 112 |
List of tables

Table 1: Threat/risk matrix, road transport using Eurowatch data 2002-2009, 4 represents the highest risk (Robinson, 2009) ................................................................. 7

Table 2: Worldwide terrorism by targets 2006, 2007; * 2007 numbers only the first three quarters (MIPT Terrorism Knowledge Base in Security Management Issues: 2007 November and 2008 April) .................................................................................................................. 10

Table 3: Worldwide terrorism by tactics 2006, 2007 (MIPT Terrorism Knowledge Base in Security Management Issue: 2008 May) .......................................................................................................................... 10

Table 4: Worldwide terrorism by region 2006 (MIPT Terrorism Knowledge Base in Security Management Issue: 2007 October) ........................................................................................................ 11

Table 5: Claims statistics LSP, claims proportions, 2006-2007 ......................................................... 13

Table 6: Claims statistics LSP, claims proportions, 2006-2007, simplified .................................... 13

Table 7: Value and number of incidents (road transports), reported to TAPA, September 1999 to December 2000 (Winterburn, 2005) ...................................................................................... 14

Table 8 Value of loss per country (road transport), reported to TAPA, September 1999 to December 2000 (Winterburn, 2005) ........................................................................................................ 15

Table 9: Yearly summary of incidents and value of losses (Winterburn, 2005) .................. 15

Table 10: Distribution of theft methods over four years (Winterburn, 2005) ................................ 15

Table 11: Sum of product types over four years (Winterburn, 2005) ........................................... 16

Table 12: Reported thefts in transport through the E18 corridor 2003-2005 (NCO, 2006) ... 17

Table 13: Table of differences between holistic and reductionist approaches (White 1995). 41

Table 14: Supply chain system with risk description and risk management strategies (based on Juttner et al., 2003; Peck, 2008) ....................................................................................... 44

Table 15: Classification of the appended papers ........................................................................ 66

Table 16: Empirical data sources used in this thesis ................................................................. 70

Table 17: Relationship between the papers and the research questions ..................................... 71

Table 18: Different authors’ roles in appended papers ............................................................ 71

Table 19: The result of the appended papers and the research questions ............................. 85

Table 20: Transport mode theft characteristics .................................................................. 86

Table 21: Comparison of losses at retailers and distribution in Sweden 2007 ................. 139
1. Introduction

This thesis examines the subject of antagonistic threats to supply chain performance, limited to the transport network that intertwines the supply chains. Chapter 1 introduces the research questions, their motivation, the scope, and the delimitations of the study. This chapter presents a definition of antagonistic threats within the scientific field of supply chain risk management. Chapter 1 also presents official criminal statistics and reports regarding the problem with primarily cargo theft from the transport network in both Europe and Sweden in addition to the smuggling of goods by abusing the transport network. Finally, it introduces the antagonistic threat from non-economical driven crimes such as terrorism.

1.1. Background

The foundation of trade is the ability to move or transport a product from the source to the customer and still make a profit (Landes, 1998). The foundation of businesses can be described with the two fundamental major problems—finding or creating demand and how to supply it. According to Smith (1776), the correct price for a product is found where supply and demand meet or the “real price of every thing ... is the toil and trouble of acquiring it” This statement assumes that each actor in the market has equal information about the product (information symmetry) and that prices and wages as perfectly flexible; this type of market is called perfect and is only a theoretical assumption (Mankiw, 1992). Both prices and wages have a certain degree of stickiness, according to Keynes (1936). This stickiness implies that the interaction of "aggregate demand" and "aggregate supply" adjusts slowly (Mankiw, 1992). The knowledge of information about the product between the buyer and seller can be described normally through degrees of asymmetry, affecting the transaction cost (Williamson, 1991; Bajo et al., 2006). This gives the market a semi-flexible price and supply mobility and makes up a continuum of several equilibriums that together describe the market as a whole. Therefore, the relationship between macroeconomics and the underlying microeconomic behaviours assumes a form qualitatively different from microeconomic models (Keynes, 1936). The use of complexity theories in economics leads to the old idea of market equilibrium is altered. The complex economical theories uses the old economical theories and adds strategies, human behaviour and other types of feedback ideas which then affects the economics equilibrium. In general terms the complex economical theories can be described as instead of rational in attend, being closely to rationality and thereby behaving in short-terms unpredictable (Gallagher et al., 1999). The system attributes are more than just the sum of its components, but depend on the characteristics of and interplay between these components. This creates a comprehensive understanding of component characteristics and their interrelationships together with the holistic system approach that are necessary to describe and fully understand the system behaviour. This thesis is based on this approach.

Supply and demand are two sides of the same coin in business; by controlling either supply or demand, one organisation can increase its ability to affect the price of a certain commodity within a certain geographical area (Mankiw, 1997). Normally the supply side is considered easier to control than demand. The supply side can be described as the question of how to produce or acquire parts for the complete product. The business world has many laws and regulations that fluctuate from time to time and place to place. On both sides of the law, businesses face the question of whether to produce or acquire goods to meet customer demand (cf. Smith, 1776). Figure 1 illustrates the produce/acquire dilemma from a legal point of view.
Figure 1: The produce/acquire matrix and legality of the business

Whether a company decides to produce or acquire can be seen as a risk assessment strategy based on a cost-benefit-analysis. According to Mankiw (1992), the central principle in microeconomics is that all households and firms optimize. “They do the best they can given their objectives and the constraints they face” The optimize principle and the risk assessment strategy aim to fulfill Mankiw’s (1992) statement of an internal profit/risk cost optimum. It is normally agreed that a larger business risk requires a larger profit, but in real life risk apprehension differs (Cleary et al., 2006). Normally business risk is referred to as the likelihood combined with the economic impact of a certain negative incident/source (Wang et al., 2000). Therefore, business risk can be regarded as a cost (risk cost) and consequently be understood with the same tools and theories as other costs (Colbert, 1991; Doff, 2008). The search for minimizing personal business risk always has been a part of doing business (Waters, 2007). Risk management is, therefore, the pursuit of the optimum balance between potential profit and risks (Doff, 2008). This means that risk management includes all activities normally referred to as management (Hardy, 1999).

The World Trade Center attack in 2001 changed the world and with it the conditions for logistics worldwide (Sheffi, 2001; Burke, 2005). The aftermath of the attack brought needed attention to the vulnerability of modern supply chains. This vulnerability can in many cases be described as “unwanted effects” in the supply chain caused either by internal or external forces that create disturbances larger than the supply chain is designed to handle. The disturbance can be either unintentional or deliberate and legal or illegal. This thesis addresses the antagonistic threats that cause disturbance in a supply chain.

1.1.1. Definition of antagonistic threats

Business risk is commonly defined as the likelihood of a negative incident combined with the economic impact of that incident/source. The entire risk handling process is referred to as risk management. The usage of risk management tools and processes within the scope of logistics and supply chain management is defined by Norrman and Lindroth (2002) as:

<table>
<thead>
<tr>
<th>Acquire</th>
<th>Produce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchase of wholesale goods</td>
<td>Manufacture</td>
</tr>
<tr>
<td>Theft or purchase of wanted</td>
<td>Manufacture of counterfeit</td>
</tr>
<tr>
<td>products</td>
<td>products / non-intellectual</td>
</tr>
<tr>
<td></td>
<td>rights</td>
</tr>
</tbody>
</table>

Legal                         Illegal

Figure 1: The produce/acquire matrix and legality of the business
Supply chain risk management is to [collaborate] with partners in a supply chain applying risk management process tools to deal with risks and uncertainties caused by, or impacting on, logistics related activities or resources.

According to Juttner et al. (2003), supply chain risk management is defined as “the identification and management of risks for the supply chain, through a co-ordinated approach amongst supply chain members, to reduce supply chain vulnerability as a whole”.

The basic construction of the elements in the term supply chain risk management can be illustrated (Figure 2). The core activity is the transaction process of a risk source to a risk consequence within the context of a supply chain with different management strategies to mitigate risk consequences. Therefore, supply chain vulnerability is defined as: “the propensity of risk sources and risk drivers to outweigh risk mitigating strategies, thus causing adverse supply chain consequence” (Juttner et al., 2003).

![Figure 2: Supply chain risk management — basic Constructs (Juttner et al., 2003)](image)

Both the above definitions and the basic construction of the term supply chain risk management are general and therefore consider all risks and uncertainties without exception. This thesis addresses a limited array of risks and uncertainties that are defined as antagonistic threats. Antagonistic threats and other risks and uncertainties are demarcated by three key words: deliberate (caused), illegal (defined by law), and hostile (negative impact, in this thesis, for transport network activities). This establishes the following definition which is used throughout this thesis:

*Antagonistic threats are deliberately caused illegal and hostile threats against the planned or wanted logistics process, function, and structure.*

Based on this definition, the core element for antagonistic threats are motivated perpetrators with hostile intentions toward the object and/or third party that violate an international, country, or local law. The antagonistic threat is therefore a crime and can be understood with the use of theories from criminology, or the scientific study of crime. According to several authors (Stock, 1997; Arlbjörn et al., 2002; Solem, 2003), criminology is interdisciplinary research of the history and future of logistics, and this thesis follows this tradition by using theories from criminology to strengthen the field of supply chain risk management. This mix of theories also challenges the predominant research approach in logistics related to tangible
artefacts (Gubi et al., 2003), and human intervention or influence to a smaller extent (Aastrup et al., 2008). The reason for this approach is that violation of law is considered a human attribute. Criminology distinguishes three elements of a crime that are present in all sorts of crime ranging from occasional violence to advance and complex economic crimes (Sarnecki, 2003; Sherman et al., 1989). The elements are:

1. Motivated perpetrator
2. Suitable object
3. Lack of capable guardian

All three elements are important to understand each individual crime. The three elements are described in this thesis as:

1. Motivated perpetrator
2. Object (goods and equipment flowing through the transport network)
3. Lack of security

These three different elements can further be defined as:

**Motivated perpetrator:** The perpetrator is an individual that, based on the outcome of the decision process (Chapter 2.11.5), commits a certain action or prepares for a certain action that is prohibited by locality or country of international law. The perpetrator can be modelled with two different categories depending on how decisions are made by each individual, namely rational choice theory (also known as the economical man theory) or determinism (Chapter 2.11.1). Both types are only possible in theory and therefore can the general description of human behaviour be described as acting rational on the margin or limited (by circumstance, choice or mixture of both) rational choice.

**Object:** The desirable outcomes or objects for the motivated perpetrator differ greatly depending on the motivated perpetrator’s decision process. Normally is it suitable to describe the object as the primary or direct reason for the action, but also as secondary or indirect reasons. The primary objects can be shipped products, resources used, infrastructure, or even the media attention an attack will receive (terrorist attacks). It is in the relationship between object and motivated perpetrator that the categorisation of the antagonistic threat is found (Chapter 1.1.3-1.1.9)

**Lack of security:** The preventive measures that can be induced to alter the motivated perpetrator’s decision process are called security. If the security measures are considered insufficient by the motivated perpetrator, then there is nothing to prevent the crime.

This leads to the special case of crimes against logistics functions and processes which are defined as antagonistic threats.

1.1.2. **Antagonistic threats against the transport network**

The theoretical contribution of this thesis is the use of criminology theories in supply chain risk management to handle antagonistic threats against the transport network. The model this thesis uses is presented in Figure 3, where antagonistic threats are shown using the theory of element of crime from criminology. The antagonistic threats address the transport network which is described with theories from logistics and supply chain management. Finally, the
handling or managing antagonistic threats is described from a risk management perspective. Basically, there are four different strategies or methods in order to handle the risks (Wang et al., 2000); 1) Avoidance: Discontinue the practice that creates the risk, 2) Mitigation: Implement strategies to reduce the impact, 3) Transfer: Transferring the risks with contracts or insurance policies, and 4) Acceptance: Live with the risk. The elements presented in Figure 3 form the theoretical backbone of this thesis.

According to Landes (1998), all human driven forces (the core of the human motivation and salvation) can be simplified through God, gold, and glory. They all play a roll in human activities, but the strongest is gold because it pays the bills, equips organisations, tempts, and soothes human flesh (Landes, 1998; cf. Smith, 1776; Mankiw, 1997). This general description of human driving forces is simplistically reformulated into two basic types of antagonistic threats to the transport network - economically driven and non-economically driven crimes. This classification may seem too simple at first, but in reality tends to be valid more or less for all crimes, even against the transport network. Therefore, the classification refers to the primary reason/motivation behind the perpetrator’s actions. The economically driven crimes can be subdivided further into theft and smuggling. The theft problem is aimed directly toward the logistics activities while the smuggling abuses the transport network for illegal purposes. The non-economically driven crimes are called terrorism normally, which clearly states that the primary reason/motivation behind the actions are based on political, ideological, or religious ideas or other non-economical philosophical ideas or teaching. Terrorism is defined by TE-SAT (Europol, 2007) as, “not an ideology or movement, but a tactic or a method for attaining political goals.”
This simplification of antagonistic threat characteristics should be seen as more of a grey-scale than a true classification. Some perpetrators are after the thrill and excitement the accomplishment of the crime will give them. These perpetrators are referred to normally as action junkies, and the action part is a non-economically driven motivation for the crime. The action junky perpetrator may very well be (primarily) after the money or products, but gets adrenalin rush during the realization. A similar type of perpetrator is the attention seeker. At first, attention seekers appear as terrorists. However, they do not seek attention for political, ideological, or religious ideas, but rather for themselves. The driving force is similar to the action junky but instead of getting the rush during the crime these perpetrators get it afterward when they see themselves in the newspapers or on TV. Better security attracts the action junky and the attention seeker, instead of discouraging them from the potential crime. For more perpetrator characteristics, see Chapter 2.10. Several authors (Anderson, 2007; Badolato, 2000; Tarnef, 2006) claim that the sentences for cargo crimes are too soft and that increasing punishment will deter potential perpetrators. This will be addressed in Chapter 2.10.

The problem with cargo crimes is complex and different methods have different impacts on the problem, depending on which type of cargo crime needs to be prevented. The positive consequence of the “war against terrorism” is that old fashioned cargo crimes have become harder and riskier (Littman, 2003). There are several types of crime that can be linked to the logistics function and processes. This thesis does not address the problems from a judicial viewpoint. The commonly most known economically driven crimes are robbery, theft, burglary, pilfering, and smuggling goods or humans. There also are a number of other economically driven crimes that could occur together with antagonistic threats such as fraud, corruption, tax evasion, and money laundering (Pashev, 2007; Ksenia, 2008; Ross et al., 2007; Chong, 2003). Non-economically driven crimes include terrorism, sabotage, and different types of violence (Naylor, 2004; Burnett, 2002; Findlay, 1999; Napoleoni, 2004; Larmour et al., 2001; Clutterbuck, 1987). This thesis acknowledges the differences with regard to definition and modus for these crimes.

1.1.3. Theft of cargo, vehicles, and driver belonging

There is a significant problem with the theft of cargo worldwide. It is estimated that theft represents a loss of at least US$10 billion per year in the United States and US$30 billion worldwide (Barth et al., 1998; Anderson, 2007). These figures are calculated extraordinarily conservatively, since most cargo theft goes unreported and these figures reflect only the value of the items and nothing more (Barth et al., 1998). There are predictions that the real figures for cargo theft are either grossly underestimated or overestimated in official reports (Gips, 2006). The theft of cargo value for the European Union is estimated to be €8.2 billion annually, an average value of €6.72 per trip (EP, 2007). Gathering accurate numbers for cargo theft losses is difficult or impossible in many cases, due to limited reporting by the transport industry and the lack of a national law enforcement system requiring reporting and tracking uniformity (CEMT, 2001). Even the insurance business has problems separating fraud from real theft, but even if they had accurate numbers they would not share it with the public because of concern about trade secrets and competition. Despite these figures, cargo theft generally has a low priority status in most countries and is often perceived largely as the cost of doing business (EU, 2003).

According to the ECMT (2002), approximately 1 percent of all commercial vehicles in European countries are stolen each year. The development differs greatly between different coun-
tries in the EU. The average increase during a five-year period (1995-1999) was 20 percent. There are many reasons behind a truck theft, but they can be described basically with three main characteristics—value, cargo carrying ability, and valuable documents. The first characteristic, value, represents the truck’s value as all objects and can be sold and exchanged for money. The second characteristic, carrying ability, refers to the general propose of a truck. The vehicle and its load were targeted in 63 percent of the attacks (IRU, 2008), and in 10 percent of all freight crimes are hijackings (Robinson, 2009). The truck can be stolen with the current load where the goods are the desirable object and the truck is only the simplest method to move the goods to a warehouse or to another truck for further movement. A truck also can be stolen for other criminal activities.

The third characteristic of theft problems toward freight is the attack for the lorry-driver’s private property or other types of valuable documents such as credit cards, mobile phones, and digital cameras stored in the truck during transport. The lorry-driver’s private property represents the target in 43 percent of all attacks (IRU, 2008). According IRU (2008), 17 percent of all drivers suffered an attack during the past five years, 30 percent were attacked more than once. Of all drivers attacked, 21 percent reported they were physically assaulted during the attack (IRU, 2008). According to Dillén (2006), this type of attack represents a considerable amount of the total, but nothing was stolen in 38 percent of attacks against trucks (Dillén et al., 2006). However, even if nothing was stolen it was still a crime against a part of the transport network and therefore shall be seen as an antagonistic threat. Seventy percent of attacks against road transports occur between 22:00 in the evening and 06:00 in the morning (IRU, 2008). This trend is also found in official Swedish criminal statistics (Nilsson et al., 2009). Therefore, it is possible to state that time of day plays an important role in antagonistic threats.

Regardless of which of the three characteristics of theft problems the motivated perpetrator uses, there is a number of commonly defined modus operandi or methods to attack trucks. These different modus operandi are used differently depending on where the attack is executed. The different locations are described in terms of different steps in a road transport from consignor to consignee, which starts with loading the goods and ends when unloading them. Eurowatch has developed a threat/risk matrix based on the data on cargo theft in road transports over a seven-year period (Robinson, 2009). The matrix presented in Table 1 maps modus operandi and location of attacks against each other.

<table>
<thead>
<tr>
<th></th>
<th>Hijack</th>
<th>Robbery</th>
<th>Theft from vehicle</th>
<th>Theft of vehicle</th>
<th>Fake police</th>
<th>Fake accident</th>
<th>Deception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load point</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Driving</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Insecure parking</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Secure parking</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Near end Location</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Unload point</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

*Table 1: Threat/risk matrix, road transport using Eurowatch data 2002-2009, 4 represents the highest risk (Robinson, 2009)*
A quick analysis of the matrix points out some obvious relationships. The method *fake accident* is best suited to deceive a truck driver to stop during driving and then conversion to a hijack. The same course of events can be created with the use of *fake police* tactics. The threat/risk matrix points out the most dangerous location to be *near end location* or at *insecure parking* depending on which modus operandi is considered most threatening.

The greatest source of risk for businesses is trusted insiders (Barth et al., 1998). Some authors consider insiders to be involved in approximately 60 percent of all losses (Tryon et al., 1997). According to Robinson (2009) is 65 percent of all “whole load losses” related to the use of inside information. Others claim there are no reliable figures (Muir, 1996). This is interesting when considering the fact that most countermeasures are implemented to reduce external theft (Beck, 2002). An internal perpetrator acts not randomly or in an unstructured way, but more as a response to social and environmental factors present in the work environment (Tryon et al., 1997). This will be further developed in Chapter 2.11.9.

1.1.4. Smuggling of goods

The primary target of illegal goods is the black market. The black market consists of places and situations where products with doubtful or no legality are traded for money. This market is subject to the same forces of supply and demand as legal ones (FIA, 2001). Buyers of these illegal products are everywhere (Johns et al., 2003). Statistical reports show that counterfeited and pirated items amounted to $176 billion in Europe in 2007 (Rodwell et al., 2007). According to another report from the European Commission, in 2006, nearly 3 million pharmaceutical products were found to be counterfeit (EU Commission, 2008). Product smuggling does not necessarily mean that the product is illegal everywhere. What is legal in one country can be illegal in another, which creates the possibility that the actors in smuggling can be legal companies that are trying to access a market that is prohibited for them. An example of this is Western companies that smuggled products into former communist countries during the Cold War era.

A problem linked to smuggling is the manufacturing of products without intellectual rights, or the production of counterfeited goods. Everything that has been produced can be reproduced by someone else. In terms of contraband this simply means that everything can be a counterfeited product (IACC, 2005). In order to bring counterfeited products from the production site to the end user, they may have to cross several national boundaries as well as intellectual property legislation. The counterfeiting business evolves constantly within current trends and technologies (EC-web, 2005). The production and distribution of illegal products is performed under the risk for detection and this diversity leads to a different design of the supply chain. The location of the production facilities is subject to the risk of discovery. Normally, illegal production units are placed where the risk for detection is low, in line with the normal legal business problem of where to produce according to different types of costs and quality aspects. Then, the illegal products are distributed by trade routes and port activities in the same way as legal products (Naylor, 2004). The pollution of illegal products in the legal transport network is a serious problem. The most common countermeasure against smuggling is the inspection of cargo carriers when they cross a national border. The mere existence of these inspections creates disturbances in the transport network, even if no illegal product is discovered (Fletcher, 2007). The current strategy is to prevent illegal products from entering the transport network by creating secure trade lines (Gutiérrez et al., 2007). The idea of secure trade lines is evident in supply chain security programmes such as AEO, C-TPAT, etc. This strategy also aims to reduce the custom inspection disturbances in legal business. For legal
businesses, the AEO, C-TPAT, etc., are both a global supply chain headache and a business opportunity, depending on the risk for theft and counterfeiting for that company (Holmes, 2004). One common denominator is the use of information to detect illegal products inside legal logistics and flows of purely illegal products.

Naturally, the legal business companies are not pleased with the competition from illegal actors. The striving for better business deals and the general globalization trend that started centuries ago led to an embedding of illegal actions within legal markets (Naylor, 2004). This implies that the old black markets have been integrated with legal transactions and the markets today can be described as containing every shade of gray when referring to the legality of the markets as a whole (Naylor, 2004).

1.1.5. Terrorism threats

The word “terror” is a Latin word meaning “to frighten.” Consequently, a terrorist is a person that intends to frighten others through fear. The term terrorist-terrorism is itself controversial because its key signature is political and it has been used by states to illegitimize political opponents. This leads to a vindication of the state’s own use of terror against its opponents (Napoleoni, 2004). The lack of a universal definition of terrorism is one of the major obstacles for meaningful international countermeasures. The practical consequence of this is best explained with the cynical comment “that one state’s terrorist is another state’s freedom fighter” (Burns, et al., 2005). Regardless, this thesis uses the terrorism definition by TE-SAT (Europol, 2007), which says, “Terrorism is not an ideology or movement, but a tactic or a method for attaining political goals.

The World Trade Center terror attack in 2001 changed the world and the conditions for logistics worldwide. The aftermath of the terrorist attacks clearly indicated that logistics operations will suffer consequences of an attack. The logistics consequences according to Sheffi (2001) were, “It is instructive to note that these disruptions were not caused by the attack itself, but rather by the government’s response to the attack: closing borders, shutting down air traffic and evacuating buildings throughout the country Therefore, the antagonistic threat from terrorism can cause consequences indirectly for logistics operations, which economically driven antagonistic threats are less likely to involve. With this said, antagonistic threats in the form of terrorism will also indirectly affect the financial market (Johnston et al., 2006; Lowe, 2006). The effects from attacks will fluctuate depending on factors such as the nature of the attacks, the multiplier effects, the type of policies adopted in response to the attacks, and the resilience of the markets (Bruck et al., 2004).

Johnston and Nedelecsu (2006) state that, “over the longer term, there is a question of whether the attacks can have a negative impact on productivity by raising the costs of transactions through increased security measures, higher insurance premiums, and the increased costs of financial and other counterterrorism regulations”. The connection between economically and non-economically driven antagonistic threats can vary and in some cases directly depend on each other, because “terrorists raise their funds through various money-making activities that may include criminal acts, such as kidnapping, extortion, large-scale smuggling, narcotics trafficking, robbery, and theft” (Financial Action Task Force on Money Laundering, 2002). The principle driving force behind a terrorist attack is normally more diverse than an economically driven antagonistic threat (Nuzzo, 2004).
The motivation for the majority of terrorist attacks is because the perpetrator intends to influence and alter the current balance of power in a certain direction (Rystad, 2006). Both the current balance of power and the potential affects on it may only be understood within the perpetrator’s own mind. Therefore, the non-economically driven antagonistic threat is more nuanced, uncertain, and harder to predict that other types of antagonistic threats. According to Sjöberg (2008) the fear for terrorist attacks is an extreme form of perceived risk. The definition of terrorism influences the difficulty to present valid statistics for the category, because one source may classify an incident as a terrorist act while another considers it to be a “regular” crime. Regardless, there are several different statistical sources that aim to describe different aspects of terrorism incidents using different variables. Three of the most common variables with regard to terrorism are presented in Table 2-4. The target for different terrorist attacks provides a good illustration of the motivation behind the actions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>264</td>
<td>141</td>
<td>379</td>
<td>249</td>
<td>1188</td>
<td>955</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governments</td>
<td>1010</td>
<td>139</td>
<td>1147</td>
<td>233</td>
<td>1615</td>
<td>454</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Police</td>
<td>2013</td>
<td>533</td>
<td>3309</td>
<td>725</td>
<td>6091</td>
<td>1417</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private citizens &amp; property</td>
<td>1273</td>
<td>1245</td>
<td>4681</td>
<td>2476</td>
<td>8184</td>
<td>4720</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religious figures/institutions</td>
<td>462</td>
<td>519</td>
<td>561</td>
<td>3334</td>
<td>1141</td>
<td>7590</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transports</td>
<td>278</td>
<td>180</td>
<td>591</td>
<td>452</td>
<td>1541</td>
<td>870</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>1359</td>
<td>722</td>
<td>1402</td>
<td>1294</td>
<td>1231</td>
<td>2688</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>6659</td>
<td>3479</td>
<td>12070</td>
<td>8763</td>
<td>20991</td>
<td>18694</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Worldwide terrorism by targets 2006, 2007; *2007 numbers only the first three quarters (MIPT Terrorism Knowledge Base in Security Management Issues: 2007 November and 2008 April)

From Table 2 is it possible to conclude that transports are not the primary target for terrorism because they were only exposed to 4-5 percent of the number of incidents and roughly the same percent of fatalities and injuries. The different tactics a terrorist chooses demonstrates the main type of threat that preventative measures need to handle. The main types of tactics used by terrorist worldwide are presented in Table 3.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Armed attack</td>
<td>2620</td>
<td>1084</td>
<td>5025</td>
<td>1591</td>
<td>2446</td>
<td>914</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arson</td>
<td>140</td>
<td>44</td>
<td>4</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assassination</td>
<td>90</td>
<td>196</td>
<td>152</td>
<td>257</td>
<td>264</td>
<td>176</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barricade/hostage</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bombing</td>
<td>3346</td>
<td>1862</td>
<td>6229</td>
<td>6567</td>
<td>18132</td>
<td>16877</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kidnapping</td>
<td>358</td>
<td>198</td>
<td>487</td>
<td>188</td>
<td>57</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other/unknown</td>
<td>94</td>
<td>91</td>
<td>162</td>
<td>160</td>
<td>56</td>
<td>695</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>6653</td>
<td>3478</td>
<td>12065</td>
<td>8763</td>
<td>20969</td>
<td>18694</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The conclusion is evident in Table 3. The terrorists prefer to use bombs and armed attacks because 80-90 percent of all attacks used these tactics. Bombing causes a higher ratio of injury than the other tactics while assassinations (obvious and expected) have the highest fatality rate. The third terrorist variable is geographic because the terrorist threat is mainly linked to local/country/regional contexts. The new “trend” (post-9/11 terrorist attack) in terrorism is to transfer local terrorist contexts to a regional or global perspective. This effect is incredibly difficult to verify with statistical sources, but the terrorist threat is still linked closely to regions in the world. Table 4 presents the occurrence of terrorism in different regions.

<table>
<thead>
<tr>
<th>Region</th>
<th>Incidents</th>
<th>Fatalities</th>
<th>Injuries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>64</td>
<td>104</td>
<td>270</td>
</tr>
<tr>
<td>Eastern Europe</td>
<td>141</td>
<td>61</td>
<td>112</td>
</tr>
<tr>
<td>Latin America &amp; the Caribbean</td>
<td>152</td>
<td>149</td>
<td>157</td>
</tr>
<tr>
<td>Middle East / Persian Gulf</td>
<td>4540</td>
<td>9603</td>
<td>15814</td>
</tr>
<tr>
<td>North America</td>
<td>4</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>South Asia</td>
<td>1206</td>
<td>1877</td>
<td>3899</td>
</tr>
<tr>
<td>East/Central Asia and Oceania</td>
<td>394</td>
<td>264</td>
<td>677</td>
</tr>
<tr>
<td>Western Europe</td>
<td>152</td>
<td>6</td>
<td>35</td>
</tr>
<tr>
<td>Total</td>
<td>6653</td>
<td>12065</td>
<td>20969</td>
</tr>
</tbody>
</table>

Table 4: Worldwide terrorism by region 2006 (MIPT Terrorism Knowledge Base in Security Management Issue: 2007 October)

Table 4 clearly indicates that the main risks for terrorist attacks are in the Middle East and South Asia. One limitation of this table is that Africa has only 64 terrorist incidents while there is civil war in several African countries (open conflict or low intense conflicts). This shows the hardship separating terrorist incidents from conflict zones, even if it is only from a theoretical point of view. The general conclusion from these three tables (2-4) is that the risks from terrorists are primarily locally/nationally/regionally linked and they prefer to attack non-business related targets using armed attacks or bombs.

This thesis addresses the economically driven antagonistic threats against the transport network but acknowledges that the threats terrorist attacks represent for modern society also influence every day logistics business processes. The model presented in Figure 3 is valid for all types of antagonistic threats, but the components in the model will change based on the special type of threat analysed. The biggest difference is found in the second table of the elements of crime (suitable object) because for a non-economically driven perpetrator, the object’s symbolic value and political meaning qualify it as suitable, not its economical value (Napoleoni, 2004; Peste, 2003; Kimbell, 2002; Rystad, 2006). The modern or new thing with terrorism is not the use of violence to influence and alter the current balance of power in a certain direction. This has always been the goal with terrorism. According to Gearson (2002) is: “Terrorism in all its forms, by its very nature, an asymmetrical response to superior force, and terrorist have always used their capabilities as force multipliers – usually through the exploitation of terror. The generation of fear, in effect the use of purposeful violence as a form of psychological warfare can now be carried much further, enhanced by the modern media and the proliferation of mass media as much as by the proliferation of weapons”. The new thing with terrorism is therefore more related to development in media technologies than to vulnerabilities in supply chains. Nevertheless, terrorism is a special form of antagonistic threat that needs to be managed, in one way or another.
1.1.6. Shrinkage or loss for different actors in a supply chain

The term inventory shrinkage is the loss of products between the point of manufacturing or purchase from supplier and the point of sale. According to the report, “National Retail Security Survey” (NRSS, 2002), the average shrinkage rate is 1.8 percent of total annual sales. This means a total loss of $33.21 billion annually in the U.S. The report points out four major sources of shrinkage: employee theft, shoplifting, administrative error, and vendor fraud. Therefore, three of four sources for shrinkage are criminal actions. The losses in the European fast moving consumer goods are for 26 percent in manufacturing, 8 percent in distribution, and 66 percent in retail (ECR, 2003). Shrinkage during distribution/transport is approximately 0.14 percent of annual sales for all types of products. The report, “TAPA Loss Data Benchmark Survey 2006” (TAPA, 2006), states the worldwide loss ratio as 0.025 percent of the total revenue ($307 billion revenue and $77 million in losses). Benchmark participant loss rates varied from 0.0038 percent to 0.25 percent of total revenue. The four different reports (NRSS, 2002; ECR, 2001; ECR, 2003; TAPA 2006) indicate that the annual shrinkage during distribution/transport would be 0.025 percent to 0.14 percent of annual sales. This loss ratio is compared with the loss ratio for retailers (1.75 percent) and manufacturers (0.56 percent) (ECR, 2003).

The losses presented according the mode of transport gives the following result (TAPA, 2006): truck (74.6 percent), air (23.1 percent), rail (0.8 percent) and sea (1.5 percent). This survey indicates two conclusions. First, the risk for losses varies greatly between different modes of transport. There is no surprise that truck and air combined represent 97 percent of all losses, since they are the primary modes of transport for the survey participants, depending on their high-value goods. However, that does not explain the huge difference between the modes.

1.1.7. Insurance claims (FFL) for one of the worlds leading LSP

In the freight industry, liability insurance is designed to offer specific protection against third party claims. The key element in liability insurance is the contract between the parties involved. Contracts which specify liability between a Freight Forwarder (FF) or a Logistics Service Provider (LSP) and a cargo owner are referred to as Freight Forwarder Liability (FFL). According to Stöth (2004), the key element of all liability contracts is the usage of clear and distinct borders of responsibility. This makes it easier to establish who is responsible if something happens unexpectedly. In order to control and simplify handling customer claims for the FFL, one of the world’s leading LSPs has developed a database. Claims made on the LSP are registered in the database. This means that invalid claims also are registered. However, the FFL database provides a good indication about what causes problems for the LSP to fulfil the cargo liability toward the goods’ owners. Table 5 shows the nine different types of causes (described by the database) presented in order of occurrence of the number of claims, claims amount of compensation, and the net cost for the LSP. Due to business reasons, percentage presented. The claims database contains more than 26,000 claims annually.
The categorisation of the nine different FFL causes is done by claims managers in different parts of the worldwide LSP organisation, and therefore the same type of FFL claims may be categorised differently in the database. Reducing the categories can be done so that different types of FFL claims that refer to lost goods are combined (in one way or another). This would reduce the number of categories to five and also pinpoint the lost-ratio within the FFL. Even with this change, it is still likely that cases of lost goods will be categorised as damaged. However, the FFL-claims statistics provide a description of how an LSP experiences shrinkage in terms of claims on liability insurance. Table 6 presents the simplified FFL statistics.

Table 5: Claims statistics LSP, claims proportions, 2006-2007

<table>
<thead>
<tr>
<th></th>
<th>2006</th>
<th>2007</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Of claims</td>
<td>Claimed value</td>
<td>LSP net cost</td>
<td>Of claims</td>
</tr>
<tr>
<td>Breakage</td>
<td>86,41%</td>
<td>87,96%</td>
<td>89,67%</td>
<td>87,45%</td>
</tr>
<tr>
<td>Delay</td>
<td>0,35%</td>
<td>0,35%</td>
<td>0,00%</td>
<td>0,20%</td>
</tr>
<tr>
<td>Error and omissions</td>
<td>1,67%</td>
<td>1,93%</td>
<td>2,37%</td>
<td>1,55%</td>
</tr>
<tr>
<td>Lost part</td>
<td>6,19%</td>
<td>3,20%</td>
<td>3,51%</td>
<td>5,62%</td>
</tr>
<tr>
<td>Lost whole</td>
<td>3,57%</td>
<td>3,34%</td>
<td>4,07%</td>
<td>3,14%</td>
</tr>
<tr>
<td>Other</td>
<td>1,71%</td>
<td>3,02%</td>
<td>3,37%</td>
<td>1,95%</td>
</tr>
<tr>
<td>Theft</td>
<td>0,04%</td>
<td>0,03%</td>
<td>0,00%</td>
<td>0,00%</td>
</tr>
<tr>
<td>Traffic accident</td>
<td>0,01%</td>
<td>0,02%</td>
<td>0,00%</td>
<td>0,00%</td>
</tr>
<tr>
<td>Water</td>
<td>0,05%</td>
<td>0,14%</td>
<td>0,00%</td>
<td>0,09%</td>
</tr>
</tbody>
</table>

Table 6: Claims statistics LSP, claims proportions, 2006-2007, simplified

According the statistics in tables 5 and 6, it is no surprise if the LSPs consider breakage as the biggest source of shrinkage. These tables also show statistics on the relationship between the different years the FFL claims are fairly stable. The lost goods row indicates that the shrinkage from missing goods is approximately 10 percent of total losses. However, the uncertainty related to these statistics limits any far-reaching conclusions about the problem with antagonistic threats toward logistics activities.
1.1.8. Cargo theft in Europe

There is no complete and fully trustworthy statement about the problem in Europe for thefts of goods and smuggling in relationship with the European transport network. The knowledge of theft problems is generally considered better than knowledge of smuggling because it is more difficult to hide a theft than a smuggling attempt. In some of the European countries, up to 1 percent of cargo vehicles are stolen each year (ECMT, 2002). This demonstrates the seriousness of criminal activities within the logistics business. The problems with cargo theft, vehicle theft, theft of goods from vehicles, and theft of the entire vehicle loaded with goods have increased. It has been shown that cargo theft is a grave threat to modern trade (EP, 2007). In Europe, the theft of cargo carrying vehicles alone increased by 21 percent over a five-year period between 1995 and 1999 (ECMT, 2002). A study conducted on an initiative of 20 high-tech companies to measure the value of the stolen goods between September 1999 and December 2000 showed 150 incidents of theft, of which 25 percent were hijacks. The products stolen were all of high value, mainly computer equipment and related peripherals, or cellular telephones. The total value of known losses was 32 million Euros (ECMT, 2002).

The problem with the theft of goods during transport is also growing, according to the organisation TAPA EMEA (Technology Asset Protection Association – Europe, Middle East, and Africa). According to their figures (which are a fraction of the transport activities within Europe and only represent their members, who transport more desirable goods than in general) both the location and the mode of procedure distinguish the problem. The relationship between the stolen value and procedure is strong. Hijacks represent 25 percent of the incidents, while they represent 46 percent of the value.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Value in US$ (millions)</th>
<th>Number of incidents</th>
<th>Value/incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hijacks</td>
<td>15.8</td>
<td>38</td>
<td>410 526</td>
</tr>
<tr>
<td>Terminals</td>
<td>8</td>
<td>28</td>
<td>285 714</td>
</tr>
<tr>
<td>On the way</td>
<td>6.7</td>
<td>58</td>
<td>115 517</td>
</tr>
<tr>
<td>In parking spaces</td>
<td>3.7</td>
<td>21</td>
<td>176 190</td>
</tr>
<tr>
<td>Jump ups</td>
<td>0.1</td>
<td>5</td>
<td>20 000</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>33.9</strong></td>
<td><strong>150</strong></td>
<td></td>
</tr>
</tbody>
</table>

Table 7: Value and number of incidents (road transports), reported to TAPA, September 1999 to December 2000 (Winterburn, 2005)

If these numbers are presented in relation to the country where the incident occurred, the following view of the problem is obtained.
Table 8 Value of loss per country (road transport), reported to TAPA, September 1999 to December 2000 (Winterburn, 2005)

Tables 7 and 8 present a picture of theft incidents in Europe, targeting companies that trade in high value products. Indirect costs or losses such as customs duty and taxes shall be added to the value or direct cost in the above table. More recent numbers from TAPA EMEA present a better picture of the theft problem in Europe.

Table 9: Yearly summary of incidents and value of losses (Winterburn, 2005)

A presentation of these incidents according to modus operandi (criminal method) gives the following result.

Table 10: Distribution of theft methods over four years (Winterburn, 2005)
The table below represents the items stolen most.

<table>
<thead>
<tr>
<th></th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers</td>
<td>34</td>
<td>38</td>
<td>56</td>
<td>47</td>
</tr>
<tr>
<td>Mobile phones</td>
<td>10</td>
<td>14</td>
<td>27</td>
<td>19</td>
</tr>
<tr>
<td>IT Components</td>
<td>22</td>
<td>49</td>
<td>34</td>
<td>29</td>
</tr>
<tr>
<td>IT Peripherals</td>
<td>12</td>
<td>34</td>
<td>50</td>
<td>27</td>
</tr>
<tr>
<td>IT Supplies</td>
<td>2</td>
<td>3</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Various IT (Mixed)</td>
<td>9</td>
<td>11</td>
<td>35</td>
<td>42</td>
</tr>
<tr>
<td>Consumer electronics</td>
<td>11</td>
<td>33</td>
<td>57</td>
<td>57</td>
</tr>
<tr>
<td>(non-IT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-electronic</td>
<td>12</td>
<td>25</td>
<td>49</td>
<td>63</td>
</tr>
<tr>
<td>Cash/Bullion</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Unspecified</td>
<td>3</td>
<td>25</td>
<td>16</td>
<td>48</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>118</strong></td>
<td><strong>234</strong></td>
<td><strong>334</strong></td>
<td><strong>344</strong></td>
</tr>
</tbody>
</table>

*Table 11: Sum of product types over four years (Winterburn, 2005)*

The numbers presented in tables 9, 10, and 11 should be viewed with the knowledge that the actual number of members in TAPA EMEA have increased from 2001 to 2004. Despite that, the picture presented in Table 10 is a representative image of the problem with cargo theft in Europe. The conclusion based on the reports from TAPA regarding theft of goods from their members in Europe in 2004 is that the problem has moved from the terminals to the links between terminals, or in this case road transport in general.

“Organised theft of commercial vehicles and their loads in the European Union” (EP, 2007) states the cost for cargo theft in the EU as “the total loss of value can be estimated at more than €8,2 billion each year. Of this amount about €450 million is not declared by the transport operators. If the loss value is related to the number of loaded trips, a value of about €6,72 per trip results”. As always, these numbers should not be taken as absolute regarding antagonistic threats, but the numbers presented in this report have more credibility than normal for this type of information. The report states that 41 percent of all incidents occurred during the driving phase of the transport while nearly 60 percent occurred during a stop. The two most commonly used methods are either threats toward the driver or tearing up of the canvas of the load unit. In 15 percent of incidents trucks are stolen with the goods, and another 15 percent is hijacking and robbery. According IRU (2008), the direct cost for an attack is approximately €25000 per attack, including theft of vehicles, load and the driver’s personal belongings.

The UK home office presented its cargo theft situation in 2007 in “TruckPol Annual Report 2007” (TruckPol, 2007). Cargo theft risk is higher in UK compared than the rest of the EU (EP, 2007), with an average loss per incident of €47,146 (TruckPol, 2007). This cost increased 14.6 percent from 2006. The classification of the 2,284 recorded cargo thefts during 2007 was as follows: truck theft (51 percent), theft from truck (28 percent), attempted theft (7 percent), hijack and attempts (4 percent), deception (2 percent), theft (other) (7 percent), warehouse (1 percent). Of the stolen trucks, almost half were recovered within 48 hours. This report focuses on trucks as the primary target, but presents a list of preferred goods similar to the results in Table 11, with the difference that high-tech products have become more interesting to steal. The same trend is found in Eurowatch statistics (Robinson, 2009).
1.1.9. Cargo theft in Sweden

“Att säkra godsflöden” (“To Secure Cargo Flows”) (NCO, 2006) contains a survey of reported thefts (Swedish crime code 0876, 0883, and 0821) through the E18 corridor in 2003-2005. This survey reported all crime for the relevant crime codes; only those reports that referred to a crime within the transport business and near the E18 motorway are presented in Table 12.

<table>
<thead>
<tr>
<th>Police district</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stockholm</td>
<td>546</td>
<td>412</td>
<td>176</td>
<td>1134</td>
</tr>
<tr>
<td>Västmanland</td>
<td>33</td>
<td>27</td>
<td>25</td>
<td>85</td>
</tr>
<tr>
<td>Örebro</td>
<td>30</td>
<td>32</td>
<td>8</td>
<td>70</td>
</tr>
<tr>
<td>Värmland</td>
<td>49</td>
<td>30</td>
<td>25</td>
<td>104</td>
</tr>
<tr>
<td><strong>Sum</strong></td>
<td><strong>658</strong></td>
<td><strong>501</strong></td>
<td><strong>234</strong></td>
<td></td>
</tr>
</tbody>
</table>

Table 12: Reported thefts in transport through the E18 corridor 2003-2005 (NCO, 2006)

The lack of reliable and comprehensive official criminal statistics on crime against the logistics business became obvious for the police authority in the southwestern Sweden in late 2006. A project was launched to verify and compile all reported thefts and theft attempts and educate police officers to improve the quality of future crime reports. Since early January 2007, there have been two unique crime report crime codes for crimes against the logistics business, namely 9803 (theft of a cargo carrier) and 9804 (theft of goods from a cargo carrier). There were 2377 (2007) and 2140 (2008) reported crimes against transports in Sweden (Nilsson et al., 2009). The attacks occurred mainly along the major roads and during night time. The most palpable findings in the official Swedish criminal statistics for freight related crimes is the 81 percent of all reported crimes attacked unprotected lorries or trailers (Nilsson et al., 2009). There was a little reduction in number of stolen lorries during 198 (2008) from 216 (2007) but the number of non-recovered lorries was double to 26 (2008). The development for the theft of trailers is increasing from 105 (2007) to 135 (2008) where the number of non-recovered trailers increased by 25 percent to 25 (2008) (Nilsson et al., 2009).

Southern Sweden is more exposed to crimes against the logistics business (CargoNet, 2007; Dillén et al., 2006; Nilsson, 2008) than other parts of Sweden. The location of the attack against the flow of goods follows the overall movement of goods. Places for the attacks are terminals (foremost in bigger cities), resting places, parking lots, and industrial estates. A brief analysis of the location of the reported crimes (Swedish crime code 9804) is that it follows the main roads (Roads E4, E6 and E20) in southern Sweden. This is not a surprise since the bulk of road transport in Sweden follows these roads.

Appendix D contains a cost calculation for cargo theft in Sweden. These calculations should be seen with a holistic perspective. It is only when they are used together that they contribute to stipulating cargo theft costs. Also, the cost calculation is based on official data which omits a large number of unrecorded cases, limiting the trustworthiness of the calculation. Therefore, earlier cost estimations for cargo theft in Sweden do not present this statistical data that supports the argumentation for a certain Swedish cargo theft cost.

17
1.2. **Purpose**

The aim of this thesis is to highlight the risk of antagonistic threats against the transport network and the management of these threats. The research is intended to define different methods, and demonstrate the benefits and drawbacks of using these methods to manage antagonistic threats against the transport network. The transport network is used in this thesis as the general term to describe different types of transport and freight activities that connects the world’s supply chains. This is achieved through several independent studies (papers) presented within a frame of reference consisting of theories from supply chain management and introducing criminology theories into the field of logistics research. This thesis uses four research questions to fulfil this purpose.

1.3. **Scope**

This thesis has the general scope of providing a theoretical model to understand and manage antagonistic threats against the transport network.

1.4. **Limitations**

This research is heavily influenced by a system-theoretical approach with a holistic view instead of the characteristics of different parts. The context of this thesis is logistics and supply chain management and the boundaries are the antagonistic threats against different elements/functions of the global transport network. The main focus of this thesis is managing antagonistic threats against the flow of products through the international transport network. The research is based on an abductive research approach using theories from supply chain management and criminology to form a new framework to study these threats (Figure 3). The transport of personnel is outside the range of this thesis, but it is possible to use the results of this thesis to describe and understand the risk for antagonistic threats against personal transports, with some adjustment to the model in Chapter 6.3.

1.5. **Antagonistic threats as a wicked problem**

Logistics problems are typically classified as tame problems (Conklin, 2001), recognized as (Ritchey, 2008):

- has a relatively well-defined and stable problem statement.
- has a definite stopping point, i.e., we know when a solution is reached.
- has a solution which can be objectively evaluated as right or wrong.
- belongs to a class of similar problems which can be solved in a similar manner.
- has solutions which can be tried and abandoned.

Normal logistics issues such as efficiency in production or cost efficient distribution setup are easily associated as tame problems according to Ritchey’s classification (2008). However, antagonistic threats against the transport network do not fit the description of a tame problem. The opposite of a tame problem is a wicked problem, which Ritchey defines as ill-defined, ambiguous, and associated with strong moral, political, and professional issues (2008). Also, these problems are strongly stakeholder dependent and the description of the problem constantly changes because it consists of a vast range of complex and interacting components evolving in a dynamic context.
According to several authors (Rittel et al., 1973; Ackoff, 1974; Rosenhead, 1996; Navarro et al., 2008; Mainelli, 2008; Ritchey, 2008) the term “wicked problem” is applicable if the problem is applied to issues or challenges that cannot be solved through traditional linear and analytical methods. Wicked problems tend to be difficult to define and lack a clear endpoint. A wicked problem depends on stakeholder judgments and interpretation. According to Rittel et al. (1973), a wicked problem is unique because there are no solution principles that can be drawn from other wicked problems. Rosenhead (1996) suggested the following criteria for wicked problems:

1. Accommodate multiple alternative perspectives;
2. Function through group interaction and iteration;
3. Generate ownership through transparency;
4. Facilitate a representation of the solution space;
5. Focus on relationships between alternatives rather than continuous variables; and
6. Concentrate on possibility rather than probability.

The nature of a wicked problem is best described as “any solution, after being implemented, will generate waves of consequences over an extended – virtually an unbounded – period of time. The next day’s consequences of the solution may yield utterly undesirable repercussion” (Rittel et al., 1973). The statement clearly demonstrates that a wicked problem has multiple stakeholders, competing interests, multiple fairly incompatible goals, and no universal solution (Peck, 2008). Therefore, antagonistic threats against the transport network are a wicked problem and it is essential that to understand the context to understand the problem.

The recognition that antagonistic threats against the transport network are a wicked problem verifies the research questions from the background and theoretical framework. This is done to place or relate the research questions closer to the context. As shown through the wicked problem approach, the answers may contain competing and/or incompatible parts which depend on the perspective or viewpoint at the moment. According to Rittel and Webber (1973), the key to a wicked problem is to understand its context through different solution concepts. This thesis presents antagonistic threats by describing their context through solution methods. A wicked problem is continually evolving and mutating, and the solution is strongly connected with better or worse instead of right or wrong (Ritchey, 2008), which is normal in logistics research.

This idea challenges the mechanic and deterministic view on problems that dominate logistics research (Aastrup et al., 2008). This research aims not to establish a causal relationship between various stages in the material flow which depend on a deterministic view of problems, but instead presents multiple case studies that together are valid for the problem in a more qualitative nature (Ellram, 1996). The wicked problem classification instead presents a context in which the problem can be understood.

Most important to understand is that antagonistic threats against freight always have been a feature in business and politics. This clearly demonstrates that there is no universal solution to the problem. Even if the stakeholders involved use similar methods to manage antagonistic threats, the effects and consequences of these preventive measures will differ because of the various functions and goals of the stakeholders.
1.6. Research questions

This thesis addresses the wicked problem of antagonistic threats against the transport network with four research questions that are closely linked to the context of the problem. This chapter presents the four research questions with close links to the problem background (Chapter 1.1) and then again in Chapter 2.12 with relationships to the theoretical framework. This relates the research questions to the practical background and theoretical frame of reference.

The empirical findings of this thesis together with the theoretical framework and the description of the problem background are the three main reasons for the high reliability of the results of this thesis. The empirical findings are mainly presented in the appended papers (Chapter 4) and analysed in Chapter 5 with regard to the research questions. It is of utmost importance that the research questions are presented distinctly and in close relation with the frame of reference to elucidate their role in this thesis as well as their contribution to its reliability. Figure 4 presents the four research questions in the main model for this thesis: antagonistic threats against the transport network.

![Research Questions Diagram](image.png)

Figure 4: The relationship between the frame of reference and the research questions

The research questions will be considered as four sides of the same coin. Their combination provides the results of this thesis.

**RQ 1 What are the characteristics of antagonistic threats against the transport network?**

From the description in Chapter 1.1, it is possible to conclude that the characteristics of antagonistic threats against the transport network can be explained with the three elements of crime within the unique context of logistics operations.
RQ 2 How are these antagonistic threats organised and managed today?

The occurrence and impact of antagonistic threats needs to be managed to reduce the costs for the actors involved. Since the typical definition of business risk is the likelihood of a certain negative incident/source combined with the economic impact, the reduction of risk can focus either on reducing the likelihood or the impact. How is this achieved within the context of global transport and antagonistic threats?

RQ 3 What are the effects on the transport network with both regard to the characteristics and the management of these antagonistic threats?

The global transport network can be described in innumerable setups and designs depending on factors such as cost, time, available infrastructure and resources, etc. Therefore, the transport network is always changing according to the needs of the supply chains involved and surrounding society. The characteristics of antagonistic threats against the transport network may influence the configuration of the network, but the effects of antagonistic threats need to be managed if they are considered too costly.

RQ 4 How can antagonistic threats be managed more effectively?

This research question can be interpreted into three different ways depending on the definition of the last part of the question, more effectively. The first two meanings are linked to the cost of the problem, while the third is linked to the occurrence of the problem. The main focus of this research question is linked to the cost of the problem and the cost issue can be analysed from two perspectives. The first and most practical perspective is to break down the cost and analyse it for each stakeholder or actor in the supply chain. The second and more theoretical perspective is to analyse the total cost in a supply chain for managing the problem of antagonistic threats. The second part of the cost analysis is mainly addressed in Appendix D, but is also highlighted chapters 1.1, 6.3, and 7.1. This research question aims to answer each of the three meanings of more effectively, but the focus is set on the first two meanings, namely cost.

1.7. Outline of the thesis

This chapter presents as outline of the thesis and shall be seen as a guide to the reader. It is also illustrated in Figure 5.

Chapter 1 provides a background reflection and emphasizes the aim and practical relevance of this thesis. It presents the problem with antagonistic threats against transport activities and includes a definition of antagonistic threat. The scope of and purpose for this thesis are presented with research limitations. The research questions are also presented in this chapter from the practical description of antagonistic threats against the transport network.

Chapter 2 provides the frame of reference for the thesis. This is the theoretical foundation for the research and this chapter contributes strongly to its credibility. Also, the research questions are verified from a theoretical perspective in this chapter.

Chapter 3 presents the scientific approach and its application in the research. This chapter presents system and complexity theory and elucidates the research gap this thesis aims to ful-
The chapter ends with a discussion of the validity and credibility of the research presented in this thesis.

Chapter 4 presents the results of the independent studies (papers) used in this thesis. The chapter includes a summary of the seven papers that form the basis of the thesis. This chapter also discusses how these studies are linked together and to the thesis.

Chapter 5 analyzes the independent studies used in this thesis and answers the research questions.

Chapter 6 provides the concluding discussion of this thesis.

Chapter 7 presents the conclusions of this thesis and answers the research questions presented in Chapter 1.
Figure 5: Thesis outline
2. Frame of reference

This chapter contains deeper discussions of the theories which constitute the frame of reference and how they can be extended to encompass the wicked problem of antagonistic threats against the transport network.

2.1. Components in the framework

The frame is based on theories from three different scientific areas - criminology, logistics, and risk management. The reasons for this are presented in chapters 1.1.1 and 1.1.2. The combination of theories from logistics and risk management is referred to as supply chain risk management, a part of supply chain theory. The theoretical frame of reference is illustrated in Figure 6. The term supply chain theory contains a vast range of theories from supply chain management, supply chain risk management, logistics, transport, and risk management. The interfaces between the theoretical fields are the antagonistic threat and the consequences of these threats. The research questions address these two interfaces and therefore the disturbance in the supply chain caused by antagonistic threats.

Theories from criminology

Figure 6: Presentation of the theoretical framework for this thesis
2.2. The supply chain concepts

The scope of logistics pertains to all activities from the supplier to the customer to provide the right product, at the right time and the right place (Christopher, 1998). To be successful, all aspects of operations and information need to work together. The supply chain is a network of autonomous or semi-autonomous business processes that produce physical goods or services to customers (Lin et al., 1998). These processes can be in different companies or in the same company. The framework of a supply chain has three major components, the supplier, manufacturer, and customer, and all supply chains end with the end user and begin with the preparation of the raw material. The current economic trends argue for the need for specialization instead of emphasising the need for vertical integration (e.g., economies of scale). This trend forces large organisations to rely on partners, suppliers, consultants, and other types of external firms to deliver customer value to their marketplaces. The need for coordination of processes involved and companies that deliver this value is what supply chain management (SCM) aims to solve (Samaranayake, 2005). To demonstrate the importance of SCM, Christopher stated (1992) that in the future supply chains will compete instead of single companies. According to Lambert et al. (1998), SCM can be separated into three elements: network structure, business processes, and management components. The network structure concerns organisational and geographical relationships. The business processes represent the activities in the supply chain and the management component integrates the network structure into business processes.

The effective management of the total or smaller parts of a supply chain requires integration of information and material flow (Samaranayake, 2005). Successful SCM will achieve shorter time-to-market and greater flexibility to respond to actual customer demand and keep costs down (Samaranayake, 2005).

2.2.1. Principles of microeconomics as a business description

The principles of microeconomics are valid for all business activities, regardless of the legality of the business. The simplified presentation of the business world in Figure 1 can be further explained with general principles from microeconomics. Mankiw (1997) uses 10 principles to explain why certain decisions are economically rational. They are as follows:

1. People face trade-offs
2. The cost of something is what you give up to get it
3. Rational people think at the margin
4. People respond to incentives
5. Trade can make everyone better off
6. Markets are usually a good way to organize economic activity
7. Governments can sometimes improve market outcomes
8. A country’s standard of living depends on its ability to produce goods and services
9. Prices rise when the government prints too much money
10. Society faces a short-run trade-off between inflation and unemployment

This thesis insists that these principles of microeconomics are valid and important to understand why people decide to break laws to make money. The first four principles (1–4) concern human behaviour (roughly the same principles can be said to describe organisational economic behaviour), principles 5 and 6 state that the marketplace is the place for economic transactions, and principles 7–10 explain the government’s involvement in business.
The first principle implies that people have a choice in trade. It can be simplified as follows: “Is the expected reward (profit) larger than the expected risk (cost)?” This statement also involves large portions of the third principle. The fifth principle illuminates the driving force behind trade with no linkage to law. In all these principles, the law can be seen as either a reward or a disadvantage, depending upon which side of the law the particular actor is acting. These principles provide a general understanding of mankind; trade, and expected outcomes from actions (cf. Smith, 1776). The ten principles should be seen as an invisible red thread through this thesis.

2.2.2. The market and the end user

Christopher (2005) defines the supply chain as, “The network of organisations that are involved through upstream and downstream relationships in the different processes and activities that produce value in the form of products and services in the hands of the ultimate customer.” The goal for the organisations involved is to provide the ultimate customer with the right product and the right time and place (cf. Christopher, 1998). The place for the transaction is referred to as the market. The description and understanding of the market has been in the centre of all economical research since the days of Adam Smith (1776). The market as a concept describes business transactions which includes everything from the cradle to the grave (and again, with recycling) in a product’s life. According to Smith (1776), the market and the division of work are the two key issues that contribute to a stable economy. As Smith (1776) states, “The Butcher, the Baker, and the Brewer provide goods and services to each other out of self-interest; the unplanned result of this division of labor is a better standard of living for all three”. Smith (1776) argues that the net effect of the free market would, regardless of ultimately egoistic human motives, benefit society as a whole. According to Hardt et al. (2000), Smith’s hypothesis implies that the government is minimal but effective and acts so that private and public interests coincide. This also requires that the government act rationally. The further from rational behaviour a government is, the smaller its ability to successfully balance private and public interests for the benefit of all. The primary way for the government to achieve this is through legislation and regulation, which provide the rules of the games for the stakeholders. Therefore, a violation of the law can be regarded as a threat against the government’s ability to balance private and public interests. This conclusion may provide an interpretation of a government’s involvement in all transactions. This is the wider context (environment) for this thesis (cf. Chapter 2.9.3).

The foundation of business can be described as two fundamental major tasks: to find or create demand and supply it (Mankiw, 1997). The supply side can be described further as the question of how to produce or acquire parts for the complete product while the demand side can be understood with theories from sales, marketing, and branding. The market itself can be categorised according to the legality of the products. The business world is surrounded by many laws and regulations that fluctuate from time to time and place to place. On both sides of the law, businesses face the question of whether to produce or acquire goods to meet customer demand (cf. Christopher, 2005; Smith, 1776). The market for illegal and undefined products is referred to as the black market, but can be called the gray market because customers do not know if the product is legal or illegal in many cases. These products can be genuinely branded merchandise sold through unauthorized channels, counterfeited products, stolen products, or illegal products (drugs, etc). The gray market is the main target for counterfeited products and it has become global in recent years (Myers, 1999). The gray market is subject to the same forces of supply and demand as the legal market (FIA, 2001).
The buyer of these illegal products is everywhere (Johns et al., 2003). Smuggling products does not mean necessarily that a product is illegal everywhere. What is legal in one country can be illegal in another. For cigarettes, it is estimated that 6-8.5 percent of total consumption is supplied by smuggling (Joossens et al., 1998), opening the possibility that the actors in smuggling can be legal companies trying to access a market that is prohibited to them. A problem related to smuggling is the manufacturing of products without intellectual rights or the production of counterfeited goods. Everything produced can be so again by someone else. In terms of contraband this simply means that everything can be counterfeited (IACC, 2005). In order to bring counterfeited products from the production site to the end user, they may have to cross several national boundaries and intellectual property legislation. The counterfeiting business evolves constantly within current trends and technologies. The illegal products are then distributed by trade routes and port activities in the same way as legal products (Naylor, 2004). According Antonopoulos (2007), the discourse on the gray market is filled with the idea of a criminal underworld in order to separate it from the legal/normal upper-world. In reality it is very difficult to establish the underworld/upper-world image. The legal companies naturally are not pleased with the competition from black market actors. They may not be pleased with legal competition either, but that is another question. Striving for better business deals and the globalization trend that started centuries ago led to an embedment of illegal actions within legal markets (Naylor, 2004). This implies that the old black markets have been integrated with legal transactions, and today’s markets contain every shade of gray when referring to the legality of the markets as a whole (Naylor, 2004). Legal businesses are concerned especially with the problems of counterfeit branded products and the theft of their own products. To increase the efficiency of detecting counterfeited products, legal businesses use cutting-edge technology and security actions (Sarathy, 2006).

This thesis uses the market as the place where products are exchanged for money according to the theory of supply and demand, regardless of their legality. This follows the sixth principle of microeconomics (Mankiw, 1997), “markets are usually a good way to organize economic activity. For economically driven antagonistic threats against the transport network, it is possible to supply a product at the right time and place. Christopher’s definition of logistics (2005) captures and explains the interaction between actors, stakeholders, and antagonistic threats within the market. According to Christopher (2005), logistics is, “the process of strategically managing the procurement, movement and storage of material, parts and finished inventory (and the related information flow) through the organization and its marketing channels in such a way that current and future profitability are maximized through the cost-effective fulfilment of orders”. Christopher’s definition of logistics works well within the fifth and sixth of principles of microeconomics (Mankiw, 1997) which explain the marketplace function for economic transactions. Striving for better business deals is the practical way to maximize profitability. According to Naylor (2004), this drive and the globalization trend led to illegal actions being embedded in legal markets (cf. Antonopoulos, 2007). The simplification of each actor’s driving force, which explains both Christopher’s definition of logistics (2005) and Naylor’s statement of the blending of illegal actions within legal markets (2004), is found in the first four principles of microeconomics. Therefore, Christopher’s definition of supply chains (2005) and the 10 principles of microeconomics (Mankiw, 1997) describe the actions of the stakeholders involved - regardless of their legality - to understand the wicked problem of antagonistic threats against the transport network. However, in order to fully understand the system as a whole it is important to remember that the system is more than just the sum of its parts (cf. Keynes, 1936).
2.3. System of supply chains

Logistics research usually describes supply chains with a system approach, and the context and boundaries of the supply chain are essential to understand each supply chain. This is achieved when each supply chain is separated into several subsystems that together provide a wider understanding of the context and present the necessary boundaries. According to Arnäs (2007) and Sjöstedt (2005), it is useful to separate logistics and transports from each other and instead emphasize the dialectic relationship between the terms or systems. The logistics system is constituted by three structured elements/components: products, locations, and facilities. The transport system is constituted by three structured elements/components: vehicles/vessels, freight, and ways and terminals. The dialectic relationship between logistics and transport is illustrated in Figure 7.

![Figure 7: The dialectic relationship between logistics and transport (Arnäs, 2007; Sjöstedt, 2005)](image)

The joint positions (dialectic relationship) in Figure 7 are the six diagonal elements. The goods are represented by the terms product and freight, but from different perspectives. Infrastructure is presented in two different perspectives as location and ways and terminals. The relocation of goods using infrastructure is presented as forwarding and movement (Arnäs, 2007; Sjöstedt, 2005).

The dialectic relationship between logistics and transport provides an excellent description of the supply chain content, products, and infrastructure, but lacks the organizational element and wider environment where everything acts. By adding an additional two systems to the chart above (logistics and transport), it is possible to better elucidate the context and boundaries for supply chains using all four subsystems. According to Juttner et al. (2003), it is useful to describe a supply chain as an interactive system with four different levels. The first two levels in Juttner’s description correspond to the dialectic relationship between logistics and transport while the other two levels represent the organizational structure and wider environment. This model will be presented in Chapter 2.9.3.
This thesis addresses the issue of antagonistic threats against the transport network, which means the dialectic relationship between logistics and transport is important for this thesis. The risk management strategies/tools that stakeholders can use are not limited to the dialectic relationship between logistics and transport. Furthermore, the risk of antagonistic threats is related to the supply chain’s wider environment. Therefore, the main focus is on presenting the relationship between the four subsystems of Juttner’s model and providing a better understanding of the context and boundaries with regard to the risk of antagonistic threats.

2.4. Supply chain, logistics and transport

Managing the total or smaller parts of the supply chain as effectively as possible requires integration of information and material flow (Samaranayake, 2005). Successful SCM will achieve shorter time-to-market and more flexibility to respond to customer demand while keeping costs down (Samaranayake, 2005). The purpose of the transport network is to physically move the goods within a certain supply chain to fulfil the scope of logistics. This means the transport network only physically integrates the supply chain with the fulfilment of its transport demands (Bowersox et al., 2002). Therefore, several supply chains can exist at the same time and place in the transport network. This indicates that the relationship between supply chains and transport activities would be better described with complexity theory, especially if the interactions between components are the object of the research. This idea will be addressed in Chapter 7.2.

Looking at transport from a system perspective we find that logistics has several levels. Before examining these, we should comprehend the overall logistics field. A logistics system consists of links and nodes, where nodes are geographically fixed points such as factories and terminals, while the links are the elements connecting the nodes, i.e., the modes of conveyance. The flow of materials is the first level of the system, because it is the reason for the system’s existence. Moving material from one place to another requires a flow of movable resources such as lorries, trains, airplanes, and ships. These movable resources need infrastructure like roads, harbours, airports, and terminals (Wandel et al., 1995; Ruijgrok et al., 1991).

The complexity in logistics can be explained by displaying the four flows always involved in logistics activities. The flows of material and resources are mentioned already. These two flows represent the “physical” part of logistics, but the other two flows, monetary stream and flow of information, are just as necessary to make the system work (Lumsden, 1998). The four flows of logistics need geographical fixed constructions and infrastructure to fulfil the scope of logistics. Some of the infrastructure is owned and used exclusively by one company while some is co-owned or owned by governments. The four flows of logistics and the necessary infrastructure are the five needs for logistics fulfilment. These are illustrated in Figure 8.
Figure 8: The five needs for logistics fulfilment

Further division and description of the needs - goods flow, movable resources, and infrastructure - can be done using multi-layers (Urciuoli, 2008) and introducing humans into the model. The actual design of a transport network mixes the five needs for logistics fulfilment in a unique setup. This design is conducted primarily to achieve customer satisfaction and internal efficiency. The need for customer satisfaction is the demand from the supply chain on the transport network performance and layout (Hesse et al., 2004). The internal efficiency is the way to fulfil the demand from the supply chain. Therefore, the needs from the supply chain are the most important constraint for the transport network. The transport network affects cost and throughput time, and can increase the value of the product if used smartly (Lambert et al., 1993). The internal constraints are the costs for the network and other network internal factors such as throughput time, quality, etc.

The configuration of the transport network depends on several constraints. Some of these constraints are as follows:

*Geographical distance between consignor and consignee* – The distance between consignor and consignee, which is interesting in terms of time and metric distance? Time distance is the limiting factor in most cases.

*Geographical concentration of consignors or consignees* – A geographical concentration of either consignors or consignees increases the opportunity to coordinate pick-up or delivery activities, creating economy of scale in each transport.

*Time window for pick-up and delivery* – The consignors or consignees will control the in- or outbound logistics delivery time by using time windows.

*The volume from each consignor and the volume to each consignee* – The amount of goods an actor in the supply chain ships or receive each time.

*Infrastructure* – The network of terminals, harbours, airports, roads, and railroads used during transport.

These constraints and the economy of scale have generated several transport network designs. Hesse and Rodrigue (2004) describe five typical network configurations:
• **Point-to-point distribution**: This is direct transport from an origin to a destination. The advantage of this configuration is the reduced number of reloads and the short transport time from origin to destination. The drawback is that it generates less-than-full-loads and the cargo carrier returns empty.

• **Corridor**: Corridor routes are similar to direct transport, but instead pass through terminals in high density areas. Goods can be loaded and unloaded at each terminal to increase the use of the cargo carrier.

• **Fixed routing**: The cargo carriers in this network are scheduled in advance on fixed routes. These networks tend to use circular configurations and the cargo is reloaded in the terminals from one route to another.

• **Flexible routing**: Routes between terminals are planned based on needs instead of fixed scheduling. This requires ICT (information and communication technology) to handle the unpredictability of freight demand and resource capacity.

• **Hub and spoke**: This network design requires a central node, the hub, to which all shipments are transported. The cargo is sorted in the hub and then shipped to the right terminal, the spoke. This network design is commonly used in air traffic. The hub requires a high capacity and vast amounts of resources. The major disadvantage of this design is longer lead times for delivery from consignor to consignee (Lumsden et al., 1999).

These five network configurations are illustrated in Figure 9.

*Figure 9: Freight distribution and network strategies (Hesse et al., 2004)*

All five network configurations depend on coordination efforts. The point-to-point distribution needs to be coordinated between consignor and consignee for pick up and delivery activities. The other four network designs require more coordination. This gives all the configurations a rhythm, where the rhythm for the point-to-point distribution is weakest and the fixed routing and hub and spoke configurations are distinctly scheduled. This means that the supply chain has to adjust to some extent to the transport network. This scheduling gives the transport network a routine and systematic rhythm, but inside this rhythm the transport network is always changing, i.e., locations, routes, goods, volume, etc. In reality, the five types of network configurations are used concurrently depending on customer demand and needs. The major LSPs have terminal networks that cover large geographical areas (country, region,
world, etc.). These terminals are linked by unique combinations of the four configurations (hub and spoke, fixed routing, flexible routing, and corridor), while the point-to-point configuration typically is used to solve special customer requirements for dedicated shipments.

The risk of antagonistic threats differs between the network configurations according to the elements of crime. Different types of goods/products are shipped in the different configurations depending on the demands of their respective supply chain’s requirements. The configurations have similar and different demands for preventive measures. They are similar because the preventive measures are closely linked to the terminal or mode of transport in each configuration. The difficulty occurs when linking similar preventive measures to cover the gaps between the terminal and carrier (for all modes) in such a way that reduces the risk for antagonistic threats and does not affect the logistic requirements negatively.

### 2.5. Risk and uncertainty in the supply chain

Risk and uncertainty are often seen as synonymous (Helliar et al., 2001), but risk also can be seen as the consequence of uncertainty (Lalwani et al., 2006). According to Waters (2007), the key difference between risk and uncertainty is that risk has some quantifiable measure for future events and uncertainty does not. Therefore, risks can be defined as quantifiable uncertainties. According to Bernstein (1996), the meaning of the word risk is dare. A key component of risk is choice (Khan, 2007), and therefore risk is about choice (Bernstein, 1996). This can be expressed as, “which risk do you dare to take?” The meaning of risk evolves over time and the meaning changes depending on an individual’s perception of the world (Frosdick, 1997). Therefore, risk can be said to hold both the possibility of loss and the hope of gain (Moore, 1983). Moore (1983) marks the importance of context in the perception of risk, stating, “when terms like high risk or low risk are used, the meaning commonly depends on the starting asset base and the consequences that the occurrence of the risk would have for the asset base of the individual or organisation concerned”. Mitchell (1999) takes a similar standpoint: “Risk is, therefore, defined as a subjectively-determined expectation of loss; the greater the probability of this loss, the greater the risk thought to exist for an individual”. Both authors stress the perception of risk in relationship to its surrounding as the key to understanding the meaning of the term risk.

The scientific study of the term risk began in the 17th century and was/is associated with probability theory and gambling (Frosdick, 1997). The concept of risk combines the probability and consequence of a certain event (Wang et al., 2000). Risks are typically classified in five different categories (Dowling, 2006):

1. Operational risks. These are tied to the operations of the company. Internal controls and working protocols are used to manage these risks.

2. Capital risks. These are often precipitated by strategic investment decisions such as entering a new market, building more capacity, investing in a new technology, or taking over another company. Quantitative analysis is often used to measure these risks.

3. Financial risks. These risks make it more difficult for Adam Smith’s “invisible hand” (1776) to reward the good companies and punish the bad ones (Partnoy, 2004).

4. Social risks. These involve products and services that may hurt people.
5. Intangible risks. These tend to be associated with employees (human capital), databases, trademarks, core capabilities, intellectual property (organizational capital), markets, customers, and brands (customer capital). Some of these capital stocks and risks are quantifiable and change over time, such as market share, but many are softer risks and much harder to measure, such as innovation capability and customer loyalty (Dowling, 2006).

A categorisation of business risks also needs to account for the risk for corporate scandals (Dowling, 2006). This is a result of Enron, WorldCom, Tyco, and other corporate scandals in recent years. According to Dowling (2006), this special type is driven by growth and innovation desire from top management. Growth and innovation are normally considered good for the company. Dowling (2006) states that, “Significant growth targets nearly always strain the capabilities, resources, and work processes of a company. If this strain causes something to break, then the company’s reputation is put at risk”.

This thesis addresses operational, social, and intangible risks. This does not mean the risk for antagonistic threats only can be categorised as operational, social, or intangible. For example, one consequence of a non-economically driven antagonistic threat is stock market anxiety. The aftermath of the WTC attack fits this description. The reputational risk for the stakeholders is always an element of antagonistic threat, but is mostly the indirect consequence of a fulfilled antagonistic threat. There is also a weak link between the non-economically driven antagonistic reputational risk and the seventh principle of microeconomics (Mankiw, 1997)—
governments can sometimes improve market outcomes. It is in this weak link that the development and implementation of supply chain security programmes can be understood and analysed. However, to fully understand the governmental involvement in managing non-economically driven antagonistic threats, the analysis needs to take into account political considerations and understanding. This thesis does not take this into account. The structured process of handling risks and uncertainties is called risk management. There are three core activities in risk management: identifying risk, analysing their consequences, and designing the appropriate response (Waters, 2007; McCrimmon et al., 1986; Waring et al., 1998). Risk identification can be defined as establishing possible events (quantifiable) from uncertainties, but can just as well be defined as finding risk sources or business threats. The risk identification process for a wicked problem needs to concentrate more on possibility rather than probability; therefore, risk is not quantifiable (depending on the lack of statistics). The second core activity focuses on analysing the consequences and alternative responses to possible events. The last core activity is to design and implement the proper response. This process is illustrated in Figure 10.

![Figure 10: The basic process of risk management (Waters, 2007)]
Basically, there are four strategies or methods to handle risk (Wang et al., 2000): 1) avoidance, or discontinuing the practice that creates the risk; 2) mitigation through implementing strategies to reduce the impact; 3) transfer: transferring the risks with contracts or insurance policies; and 4) acceptance, or living with the risk.

According to Christopher and Peck (2004), the sources of risk for a supply chain can be divided into internal, external, and environmental risks. Internal risks can be subdivided into process and control risks. External risks can be subdivided into demand and supply risks. Demand risks are associated with outbound logistics and uncertainty in product demand (Svensson, 2002), and supply risks are associated with uncertainty in inbound logistics (Zsidisin et al., 2000). External risks also can be defined as risk emerging from the interaction between the supply chain and its environment (Chapman et al., 2002). Sources of environmental risks are politics, nature, and social uncertainty (Juttner, 2005). Internal supply chain risks come from a lack of visibility and ownership, self-imposed chaos, the misapplication of just-in-time logistics, and inaccurate forecasting (Chapman et al., 2002). Figure 11 illustrates the relationship and interdependency of the five sources of supply chain risk.

![Figure 11: Sources of supply chain risks (Christopher et al, 2004)](image)

This figure shows that the demand and supply risk addresses disturbance in physical distribution through in- and outbound logistics activity. Risk consequences or the disturbance can be amplified or absorbed by supply chain control mechanisms such as batch sizes, inventory safety margins, decision rules, and policies regarding order quantities (Juttner, 2005). High impact consequences also can be reduced by creating redundancy in the supply chain by using two or more suppliers or transport routes for each component (Sheffi, 2001). A disruption in either inbound or outbound logistics can affect the overall performance of the supply chain. Generally the supply chain is more vulnerable to disruption in inbound than outbound logistics (Svensson, 2002). The impact of a disruption varies, depending on the share of the total amount of inventory affected; a larger share means a more serious consequence (Giunipero et al., 2004).

The five sources of supply chain risk provide only a general description of risk and from which direction they come in a supply chain. The term “sources” does not refer to the actual cause of the incident. Risk refers to the probability of an event and a negative economic impact of that event. The risk is the expected value of an issue or event. With this said, the discussion of risk in the supply chain is a good way to describe negative effects in the chain. Juttner (2005) states that risk taking is perceived as an inevitable aspect of supply chain management. Taking risks is not the same as controlling and managing risk to an acceptable level.
2.6. Supply chain vulnerability

Historically, security and vulnerability within the supply chain were largely neglected until the terrorist attack on the World Trade Center. The subjects of supply chain security and vulnerability finally are being given the attention they need as they pertain to terrorist attacks. This vulnerability can, in many cases, be described as “unwanted effects,” or the consequence of the risk to the supply chain. Supply chain vulnerability reflects sensitivity of the supply chain to disruption (Waters, 2007). Juttner (2005) defines supply chain vulnerability as, “an exposure to serious disturbance arising from supply chain risks and affecting the supply chain’s ability to effectively serve the end customer market. According to CLSCM, supply chain vulnerability can be defined as, “an exposure to serious disturbance, arising from risks within the supply chain as well as risks external to the supply chain” (CLSCM, 2002). Both the bullwhip and the domino effect within a supply chain are considered major sources of risk which may lead to flow disturbance.

Christopher and Lee (2004 - a) suggest that the increased vulnerability in supply chains is a result of the drive for more efficiency, which also in turn increases vulnerability from disruptions or disturbances. The complexity and nature of supply chains make them vulnerable to different kinds of risks. More supply chain vulnerability is an unintentional side effect of a limited view of the types of risks that may or may not cause disruption (Waters, 2007). To reduce this vulnerability, companies must identify their internal risk and the risk derived from collaboration and linkage with other companies (Juttner, 2005). A typical response to uncertainty and vulnerability is to create flexibility in the supply chain (Prater et al., 2001). A flexible supply chain can respond to changes in internal and external factors that affect performance. The relationship between supply chain vulnerability and risk management is illustrated in Figure 12.

![Figure 12: Vulnerability of the supply chain (Waters, 2007)](image-url)

A supply chain with flexibility and the ability to respond to changes is called a resilient supply chain. Resilience is defined by Christopher et al. (2004 - b) as, “the ability of a system to return to its original state or move to a new, more desirable state after being disturbed”. Supply chain resilience includes flexibility and last minute changes to transports and production. According to Christopher and Peck (2004 - b), there are four elements that provide success in supply chain continuity management. They are:
• Risk awareness among top managers
• Risk awareness as an integrated part of supply chain management
• Understanding by each employee of his or her role in risk awareness
• Understanding that changes in business strategy affect supply chain risk profiles

The following are the four principles that characterize supply chain resilience (Christopher et al., 2004 – b):

• Supply chain (re) engineering
• Supply chain collaboration
• Agility
• Creating a supply chain risk management culture

A resilient supply chain is designed to effectively handle the risk and uncertainty that may threaten supply chain performance. Therefore, supply chain resilience can be seen as a response to supply chain vulnerability. According to Burke (2005), organisations directly affected by 9/11 immediately stopped functioning, but also, in many cases, bounced back surprisingly quickly. This demonstrates a general resilience in business, but the big question is if it is sufficient for the next grand supply chain disruption, regardless of the cause to the disruption.

The vulnerability of the supply chain is transmitted to the transport network. This depends on the simple fact that transports and freight activities physically bring the facilities of a supply chain together. Therefore, risks, uncertainties, and vulnerabilities in the supply chain and the transport network affect, contribute, and neutralize each other. The context of the five needs for logistics fulfilment, constraints, and risk for disturbance is illustrated in Figure 13.

![Figure 13: Constraints and disturbance risk affecting the five needs for logistics fulfilment](image-url)
Figure 13 shows the risk management perspective of transport from consignor to consignee and the balancing of the different constraints toward the different risks for disturbance. Further division and description of the needs, goods flow, movable resources, and infrastructure can be done using multiple layers (Urciuoli, 2008). These layers could contain stakeholders, components, and actors such as supply chain internal and external organizations and the surrounding society, including authorities and non-governmental organizations (NGOs) as well as the people in organizations. If the potential risk for disturbance is considered too high in a certain logistics setup or product flow, then the design of the system should be altered to reach an acceptable level for the mix between constraints and risk for disturbance (cf. Mankiw, 1992). The resilience of the five needs for logistics fulfilment is of vital importance for the overall supply chain resilience.

### 2.7. Supply chain risk management

Today, risk is a factor in all business functions and processes (Cavinato, 2004). Every function or process has a certain probability of not performing as planned and there is a certain consequence attached to that probability. The search for ways to minimize risk has always been a part of doing business (Waters, 2007), but minimizing the business risk often also leads to minimizing profit. Therefore, businesses pursue the optimum balance between potential profit and risk. The usage of risk management tools and processes within the scope of logistics and supply chain management is defined by Norrman and Lindroth (2002) as:

“Supply chain risk management is to [collaborate] with partners in a supply chain to apply risk management process tools to deal with risks and uncertainties caused by, or impacting on, logistics related activities or resource

According to Waters (2007), supply chain risk management is defined as:

“The overall aim of supply chain risk management is to ensure that supply chains continue to work as planned, with smooth and uninterrupted flows of materials from initial suppliers through to final customers

Both definitions clearly demonstrate the small difference between supply chain risk management and supply chain vulnerability. Several authors (Narayanan et al., 2004; Agrell et al., 2004; Chopra et al., 2000; Lee et al., 1999; Baiman et al., 2001; Ming et al., 2003; Lundin, 2008) use the term supply chain misalignments to master the dynamic in a supply chain with unnecessary vulnerability to which actors contribute by not collaborating to minimize supply chain vulnerability. The risk clauses in the contractual agreement between actors in the supply chain needs to be linked to the actor’s liability and reflect a reasonable risk/profit exposure for each actor. This idea will be addressed in Chapter 7.2.

### 2.8. Supply chain security

According to Borodzicz (2005) security can be considered as interpreted as either freedom from danger or a show of force (or strength). Both interpretation are valid for this thesis but in normal life is the the last meaning of the word security more common. The terrorist attacks at the World Trade Center and Pentagon on September 11, 2001, brought attention to security in trade, for more reasons than just the attacks. According to Closs and McGarrell (2004), three factors can be outlined: first, the globalization of world trade depends on and is generated by the free flow of people, goods, and information; second, the increasing demands from busi-
nesses for efficient supply chain operations; and third, the increasing threats of terrorist attacks. Therefore, supply chain security management can be defined as, “the application of policies, procedures, and technology to protect supply chain assets from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain” (Closs et al., 2004). The only problem with this definition is that it does not address the origin of the threat or risk. The five sources of supply chain risks provide that. Supply chain security needs to adjust its policies, procedures, and technology to protect the supply chain from all five risk sources. The flip side of supply chain security is supply chain resilience, or a supply chain’s ability to withstand and recover from an incident (Closs et al., 2004). Supply chain risk should incorporate security and resilience, where resilience also must handle a near miss incident that affects the performance of the supply chain and from which it needs to recover.

Present supply chain security research outlines several changes for how security in a supply chain should be approached. First, supply chain security should incorporate not only theft prevention but also anti-terrorism measures. Second, the focus is now on global issues and not just local or national issues (Sweet, 2006). Third, when conducting contingency planning, the concept of crisis management is to be included to obtain better resilience. Last, security is no longer an internal corporate question but rather an issue for all actors within the supply chain (Closs et al., 2004).

In the paper, “Higher supply chain security with lower cost: Lessons from total quality management,” Lee and Whang (2003) suggest that methods and ideas from total quality management can be used successfully to increase supply chain security. The main idea is the lesson from quality management that sample inspection is expensive and useless at the end of the production line. Just like in quality management, supply chain security becomes more effective and less expensive by implementing the right management approach, technology, and re-engineering operational processes. Lee and Whang state that security should be integrated throughout the entire supply chain to be successful at a reasonable price. This opinion is supported by several other authors (Borodzicz, 2005; Ritter, et al., 2007; Sarathy, 2006; Closs et al., 2004; Rice et al., 2005; Manuj et al., 2008)

2.9. Risk management and security in a supply chain context

Traditional risk management and security may appear to be congruent with each other because many security practitioners use traditional risk management methods. Traditional risk management methods are a good way to simplify and analyse complex problems such as security issues. Furthermore, they are good methods for proper allocation of limited resources to address unlimited risk sources to reduce total risk (Manunta, 1999). Most traditional risk management methods are based on statistics (achieved by various methods); therefore traditional risk management methods can give the risk manager a sense of dealing with scientific facts. Traditional risk management is derived from areas such as insurance and safety and is based on the idea that the world is mechanically predictable or deterministic. The stronger the linear relationship between cause and effect, the better the traditional risk management approach is for reducing disturbance. This base assumption leads to the idea that quality management tools are appropriate for risk management processes as well (Williams et al., 2006). The relationship between cause and effect is normally linear for process failures, while if there are deliberate actions behind the disturbance, the relationship is more or less non-linear. Therefore, traditional risk management cannot deal effectively with the dynamics of antago-
nism, the area for security. This difference is illustrated in Figure 3, where security, or a lack thereof, is found on the threat side while traditional risk management strategies (mitigation, transfer, and acceptance) are consequences of the presence of antagonistic threats.

The causes for antagonism can be described as a spiral of inputs, processes, and feedback, which explains the dynamics of antagonism. Such dynamics tend to make analysis, assessment, and decision very complex, and the world seems to be anything but deterministic (Manunta, 1999). Here, Manunta argues that security and traditional risk management oppose each other, but this is too limited a view. Both approaches aim to reduce the causes and consequences of an adverse event. By bringing ideas and mindsets from security into risk management approaches, they will be able to deal with antagonism. Understanding antagonistic dynamics is vital for an analysis of where, when, and how the protector shall be to prevent adverse events from occurring. The security version of risk management should address the dynamics of antagonism by understanding the environment or context of the threat. The context of a risk should be understood as partly perceived and partly objective, and any actor that manages the risk needs to consider its context (Waring et al., 1998). Therefore contextual risk management approaches are appropriate for dynamic risk sources, while statistical risk management approaches fit static risk sources. Contextual risk management can be seen as intelligence containing probability and effects, instead of equations, like statistical risk management (Manunta, 1999). Therefore, traditional risk management can handle risk better (quantifiable threats/problems) and security handles uncertainties better (unquantifiable threats/problems) (Waters, 2007).

The steps in a risk management process can be used for quantifiable and unquantifiable threats/problems. It is important to note whether the threat/problem can best be described as probable or possible. This difference can be demonstrated with a comparison between the risk of a terrorist attack and the risk of a cargo damage incident. The cargo damage incident is probable because it is likely that the organisation has sufficient statistics to establish a credible risk cost (Chapter 1.17). On the other hand, a terrorist attack is possible but the lack of predictability and reliable statistics makes it difficult (or even impossible) to establish a risk cost in the traditional way. However, an analysis of the vulnerability of terrorist attacks can establish the risk (as a possible risk cost) and handle it with the same risk management process (see Chapter 2.5) by accommodating multiple alternative perspectives and focusing on relationships between variables (processes etc.). This reasoning clearly demonstrates that terrorist attacks can be described as a wicked problem (Chapter 1.5).

This does not mean that traditional risk management cannot be used in security work. It simply means that it is very important to first get an understanding of the context in which the security is needed before doing any risk calculations. Where risk management is concerned about the consequence or damage combined with the probability of an event (cf. insurance principles), security is interested in why and how an incident can occur. Both approaches aim to prevent and obstruct the incident itself and limit the effects from it.

The difference between statistical and contextual risk management also can be defined by the lack of similarity or the nature of the threat from whom or what security shall protect the object. Despite that, the two concepts can be used together and in support of each other. The difference between statistical and contextual risk management can be illustrated by the differences in approach and perspective. The statistical risk approach is based on statistical information and assumes a form of randomized predictability of incidents (quantifiable threats/problems). The contextual risk management approach is based on contextual under-
standing and assumes a form of antagonistic threat and a nonlinear relationship between cause and effect (unquantifiable threats/problems). Contextual risk management is statistical risk management aimed to reduce the total risk (cause and effect).

Everything that happens in a system that causes it to vary from the ideal generates uncertainty in the system. In risk management terms, if the cause and the effect are known, the proper countermeasure or plan of action can be used (Urciuoli, 2008). Uncertainty within the system will delay the starting point for the proper plan of action. Therefore, uncertainty can be seen as a delay that should be addressed with risk management methods, as well the cause and effect of an incident. The relationship between risk management approaches, causes, consequences, and uncertainty, depending on a cargo incident, is illustrated in Figure 14.

![Figure 14: Cause/consequence matrix for cargo incidents](image)

There are three outcomes on the impact or consequence side of the risk - goods delayed, destroyed, or missing - while on the cause side there are deliberate and unintentional reasons behind the consequence. The most uncertainty-generating consequence is goods missing because it is clear with the other two consequences what has happened and the right action plan can be started. Missing goods can be due to a process failure or loss, and the goods will show up somewhere unexpected. Figure 14 does not take into account the occurrence of counterfeited products if a terrorist attack causes the consequence. Counterfeited products could be considered another type of theft, while a terrorist attack could generate all three types of consequence regardless of whether the attack and its effects were direct or indirect. Generally, the business impact will be higher if the goods are stolen or destroyed rather than delayed (depending upon the length of the delay). However, because of penalty fees between a supplier and buyer, the impact can be as serious for delay as for theft. The real problem occurs when a company’s security or risk management capability is lower than the perpetrator’s capability. The difference between these two capabilities is the window of vulnerability (Almay, 2006). A proper risk management approach aims to reduce or shut that window.
Logistics literature agrees that uncertainty should be reduced as much as possible (Nilsson, 2006). The basis of this idea is that there is equilibrium and stability in all logistics (Lambert, 1998). In other words, everything can be controlled. However, there is no stability if the risk is caused by deliberate actions. Nilsson (2004) states that logistics researchers and practitioners need to “go with the flow” with regard to uncertainty and complexity, instead of trying to remove all uncertainty. In terms of supply chain risk management, Nilsson implies that both a statistical (stable) and contextual (complex) approach are necessary to reduce total risk. According to White (1995), risk analysis can be conducted in two ways, either holistically or reductively. The difference between these two methods is illustrated in Table 13.

<table>
<thead>
<tr>
<th>Method</th>
<th>Holistic approach</th>
<th>Reductive approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue tackled by</td>
<td>Investigating the problem’s environment</td>
<td>Reducing problem into smaller and smaller parts</td>
</tr>
<tr>
<td>Approach characterized by</td>
<td>An upward movement</td>
<td>A downward movement</td>
</tr>
<tr>
<td>Simplifies by</td>
<td>Taking multiple partial views</td>
<td>Breaking down problem into simplest parts</td>
</tr>
</tbody>
</table>

*Table 13: Table of differences between holistic and reductionist approaches (White 1995)*

The holistic approach is, like the contextual approach, useful when risk arises from the environment and a greater understanding of the cause is needed to reduce the total risk. Likewise the similarities between statistical and reductive approaches are useful when the risk cause is replicable and recurrently predictable. The antagonistic threat is a risk that arises from the interior and the transport network’s environment. Therefore, the contextual or holistic approach is better than the statistical or reductive one. This thesis achieves this by focusing on the potential perpetrator and transport network based on analysis with theory from criminology and supply chain management. Also, this thesis does not attempt to break the problem down into its simplest parts, but instead performs and reports on a wide, multi-level analysis of the wicked problem of antagonistic threats in the transport network by using insights from complexity theory.

### 2.9.1. Transport and freight security

The security of freight transport was long under-developed, but since terminal security has improved, theft incidents have increased in the links between terminals (Ekwall, 2009 - a). This development is also valid from a supply chain perspective; while security in manufacturing facilities normally is focused and well-managed, the rest of the chain is without security (Purtell et al., 2006). Security during transport is necessary to prevent unwanted negative disruption in the flow of goods. The term for this prevention is transport security (EU, 2003). Transport security is the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems, and workers against intentional unlawful acts (EU, 2003). The technological development of the range and sophistication of anti-theft devices and after-theft systems is increasing rapidly (Urciuoli, 2008). Special attention is given to systems that track the goods themselves throughout transport (ECMT, 2001 - b), but applying different technological systems is only one part of transport security strategy (Tyska et al., 1983). The key issue is the successful coordination and cooperation of the actors involved in the transport. At present this cooperation is not widely developed (ECMT, 2001 - b). The lack of cooperation, together with barriers in business, is indicated by the following: underestimated risk from the haulers; different standards in technologies; insurance companies do not always give premium reductions; and technical standards do
not exist yet (ECMT, 2001 - b). These barriers and lack of cooperation can be remedied by the use of common methods or standards in transport security (Tyska et al., 1983). Together, the police and operators’ associations can disseminate advice and guidance to operators, especially about safe routes, parking areas with high security, security precautions, and appropriate equipment (ECMT, 2001 - a).

The organisation TAPA works to improve transport security through its certification programmes, Freight Security Standards (FSR) and Trucking Security Requirements (TSR). The FSR mainly addresses security issues in terminals and includes certification by an independent auditor. The FSR have three different levels, A to C, where A is highest. The FSR specify the minimum security standards for assets travelling through the supply chain and methods for maintaining those standards (TAPA FSR). The TSR, on the other hand, are certified by self-assessment and only address security issues in road transport. The TSR specify the minimum security standards for assets travelling between terminals in the transport network and methods to maintain those standards. The TSR are complementary to the FSR (TAPA). A TAPA-certified transport network is illustrated in Figure 15. The square frames represent the idea of FSR for protecting terminals, while the unprotected links illustrate the problem with introducing security with a limited view on how to protect the transport network from theft.

![Figure 15: Security in the transport network](image)

It is important to take an intermodal approach in transport security to avoid unwanted competition disadvantages between the various modes. This means also that security methods need to be internationally accepted to reduce the risk of duplication or sub-optimal solutions for security that may disrupt international trade (EU, 2003). In an intermodal transport, the first and last parts of the freight are conducted by road transport, while other modes of transport are used in between. As a consequence, road transport needs a parking place near the intermodal terminal if there is no waiting area inside the terminal borders.

### 2.9.2. Logistics security programmes

Several new security programmes were launched in the aftermath of the World Trade Center terrorist attack to protect international cargo flow from being abused for criminal (primarily terrorist) intentions without compromising supply chain efficiency. The U.S. Customs Office (DHS-web, 2007) launched several programmes such as the Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI), the 24-hour rule, etc. These security programmes address different aspects of supply chain security and target different parts of a transport chain. The link between these security programmes is that they involve all parties or stakeholders in supply chain security (Sheu et al., 2006). The effects from these programs both in order to handle security threats and their impact on different logistics processes have been addressed in a few papers (Fletcher, 2007; Gutiérrez et al., 2007; Grainger, 2007; Tweddle, 2007). Powanga (2006) states that the C-TPAT certification will probably have a negative impact, mostly on small enterprises whiles large firms instead may have the possibility to trade-off the security costs with benefits related to supply chain transparency.
Haughton (2007) demonstrates the economical and competitive advantages for large and small shippers becoming FAST-approved (Free And Secure Trade). The acquisition of the FAST status may provide shippers with faster trans-border operations and consequently a substantial advantage on the export market (Haughton, 2007). Willys and Ortiz (2004) emphasize that efficiency and security in supply chains are closely related to each others, since higher security may reduce Customs delays. The relationship between security, efficiency and custom activities is clearly found in the AEO-programme.

Other types of security programmes existed before the attacks on the World Trade Center. These programmes were designed primarily to address theft problems within the transport business (TAPA FSR and TSR, etc.) (TAPA-Web, 2008). The big difference between security programmes before and after the terrorist attacks is that afterwards, authorities (mainly U.S.) took the lead in developing and implementing these programmes. Before September 11, 2001, security was something the business itself handled. The implementation of these programmes has so far mainly occurred in the old western countries in North America and in Europe. The reasons behind this will be further addressed in chapter 7.2.

2.9.3. System of supply chain risks

According to Juttner et al. (2003), it is useful to describe supply chain as an interactive system with four levels. The first two levels in Juttner’s description correspond to the dialectic relationship between logistics and transport (Chapter 2.2) while the other two levels represent the organizational structure and wider environment. Each level is presented with elements and content descriptions of general nature and therefore should be seen as illustrative and explanatory rather than decisive. A description of the major risk sources and risk management strategies normally used to handle and minimize the risk consequences are attached to each level. In general, business considers the risk sources differently. A risk in Level 2 is considered negative while the same risk source in the perspective presented in Level 3 may entail a new business opportunity, which is normally considered good. The duality of risk perception found in levels 3 and 4 is only addressed in two of the papers (papers B and D) presented in this thesis. Table 14 presents the system of supply chain risks.

The main focus of this thesis is on levels 1 and 2, and risk is considered negative. The first two levels are described in detail in Chapter 2.3. The advantage of using four levels (or sub-systems) to describe the supply chain system is that they automatically provide a contextual understanding and boundaries for the problem of antagonistic threats against the logistics business.
Table 14: Supply chain system with risk description and risk management strategies (based on Juttner et al., 2003; Peck, 2008)

Most logistics security programmes address parts of Level 2 while focusing on infrastructure risks and therefore achieving better security in the supply chain system. Programmes such as AEO have come closer to Level 3 than other programmes by using criminal background checks (for customs crimes) for senior management of the certified company. The occurrence of criminal background checks within logistics security is a higher security requirement, but it needs more research to clarify the content, purpose, and effects of these checks (Chapter 7.2).

2.10. The insurance principle; conventions, claims, and premiums

According to Wang and Rouch (2000), risk transfer is a common strategy to control risk. The basic idea is that transferring the risk to someone else reduces personal risk substantially by using different contracts. In the freight industry, liability insurance is one of the best examples of a risk transfer strategy. The key element in liability insurance is the contract between the parties involved. Several conventions (e.g. CIM, CMR) have been developed to simplify business relationships. If nothing else is decided contractually, these conventions are contractual agreements. There also are a number of standardised contracts regarding risk regulation (Incoterms, 2000; NSAB) (Stöth, 2004). Common to these regulations is the government of compensation and responsibility between goods owners (seller and buyer) and freight forwarder actors. These conventions and standardised contracts work according to the general insurance principle.

The insurance principle prescribes that the insurance company takes over the economic impact if something happens that is covered within the insurance contract. This means the risk of this occurrence should be easy to identify, classify, and determine so the insurance company can estimate the cost related to the risk and determine the insurance premium. This premium is also accompanied by an insurance excess, giving the potential insurance buyer three components to consider: the terms, premium, and the excess of the specific insurance. Therefore,
the incentive for the individual insurance buyer is the central issue, and by extension, also the potential reduction of a potential loss (Kelly et al., 2003).

According to Stöth (2004), the key element in liability contracts is the usage of clear and distinct borders of responsibility. This makes it easier to establish who is responsible if something happens unexpectedly. The contract also should account for what this responsibility means, something the CMR convention covers. However, this means that if nothing else is agreed upon in a contract, the CMR is the rule for the risk transfer strategy. Despite that, the majority of major losses will lead to negotiation between the insurer and the client (Garrett et al., 2003). These post-contractual negotiations can be costly and lead to abuse of the insurance policy (Garrett et al., 2003).

The key element of liability insurance is that goods owner taking a majority of the risk if nothing else is decided (Stöth, 2004). The actors within a transport chain never take ownership of the transported goods, only the liability. Therefore, the goods owner, to achieve full risk transfer, needs to have property insurance, and the logistics actors need liability insurance. Of course, the differences between property and liability insurance also can be stipulated in contracts between the parties. According to Doherty and Schlesinger (2002), the marketplace for liability insurance is expanding and insurance companies are offering more professional liability insurance. This leads to the actors involved having more opinions and possibilities to optimize their risk taking.

S. Hun Seog (2006) defines the idea behind the use of insurance in business in the following way, “The optimal coverage is positive if the strategic effect is greater than the cost of insurance. The main strategic effect of insurance comes from the fact that firms purchase insurance before they produce outputs. Insurance makes firms more aggressive due to the limited risk costs of firms”.

In order to hinder an uncontrolled outcome from a specific insurance policy, it is normal to limit the potential maximum payout for a single event. Therefore, a specific insurance cover can be divided into several insurance policies with their own premium and excess based on the potential risk cost for each specific policy. One of the big advantages of this strategy is that the first insurance policy is designed to handle the most frequent payouts, while the other policies are designed to limit the single maximum payout for a specific event. These limitations can be calculated in several ways (Garrett et al., 2003).

The principle of different insurance policies also can be used to handle/transfer risk. Each insurance policy should clearly state different insurance terms. According to Spekman and Davis (2004), companies can use interruption or denial of service to transfer the risk of a potential financial loss from a security breach or other incident that normally is covered with special insurance policies. According to Garrett and Marshall (2003), a common risk strategy for an actor is to own only a minor part of the equipment they use. This depends mostly on the fact that the risk for ownership is transferred.

The usage and design of insurance policies in logistics operations needs more research to be better understood and put to more effective use (total supply chain cost) (Chapter 7.2).
2.10.1. The CMR convention

To establish clear rules and regulate responsibilities in international trade, the UN published the first edition of the CMR (Convention on the Contract for the International Carriage of Goods by Road) convention in 1956. The purpose was expressed as:

“Having recognized the desirability of standardizing the conditions governing the contract for the international carriage of goods by road, particularly with respect to the documents used for such carriage and to the carrier’s liability” (UN, 1956).

The desire to regulate the transport industry by developing a standardized set of liability regulations was obvious. The development of the CMR convention is ongoing, but the main frame was set in the first edition in 1956. The international community established regulations for sea and air freight as well. The main focus of these three regulating documents is similar—to standardize liability between the carrier, freight forwarder, and goods owner in international trade.

The CMR regulation contains 51 articles in eight chapters. For this paper, articles 17, 23, and 29 are of particular interest. These are in the fourth chapter, “Liability of the carrier” (UN, 1956). The articles describe the three main carrier and freight forwarder liability categorizations: no-liability, limited liability, and full liability. These articles govern the responsibility of the carrier regardless of whether the ground for the liability dispute is damage or theft of the goods. A general view of the content in these three articles can be expressed as, “From no liability at all, via limited liability to unlimited liability” (Spiegel, 2007). If such a thing as a normal state can be expressed in terms of carrier liability, it would be limited liability. Discussion of the carrier liability can only be theoretical in this paper. In practice, the discussion is live and often handled through courts in different countries. The general view presented in this paper is the same as the content of the living discussion.

The carrier can invoke the no-liability to a claim or the “force majeure” to the claim. According to Spiegel (2007), the precedent comes from the “Oegema/Brada,” a court verdict in 1998. This verdict shows that a “carrier must demonstrate that he has taken all measures to prevent loss, which a diligent carrier – including the persons whom the carrier engages in the performance of the contract – would take in the given circumstances” (Spiegel, 2007). The main focus here is that the carrier must have taken all measures to avoid the loss. In reality, the consequence of this principle is that force majeure is hard for the carrier to plead, even if the loss was caused by an armed robbery (Spiegel, 2007).

The opposite of force majeure, or no liability, is gross negligence, or full liability. This means plainly that the carrier compensates the full value of the lost goods to the owner of the goods. According to Spiegel, the precedent is a court verdict from 2001, “Cigna/Overbeek + Van der Graaf/Philip Morris.” The main issue was that the “Carrier acted recklessly, and with the knowledge (subjective!) that the chances that damages would occur were considerably higher than that they would not, but acted accordingly anyway” (Spiegel, 2007). The key point is that the carrier knew about the increase in risk for loss from a certain action.

In order to solve an accusation of gross negligence, the goods owner or the carrier company (the one who is first) takes on legal proceedings in one of the countries the transport passes through during freight. The prosecutor chooses the country in which they think they have the
biggest chance of winning the court’s approval. According to Spiegel (2007), there is a big difference between courts in the Netherlands and Germany regarding the possibility of having a liability issue considered gross negligence from the carrier’s side, while Germany is more likely to judge in favour of the goods owner.

2.10.2. Enhanced liability in insurance

Enhanced liability is a contract obligation between the goods owner and LSP, where the LSP have accepted extended liability for future claims payments beyond normal standards of transport law, conventions (CIM, CMR), or national standard terms and conditions (Incoterm, NSAB) for freight forwarders. This means the goods owner has transferred parts of his risk to the LSP. The same principle is valid for the contractual relationship between the LSP and a carrier company. In general, enhanced liability is a practical strategy to transfer risks from one party to another in a contract. The receiver of the enhanced liability can sign a special insurance policy that only covers the enhancement of the liability. These enhanced liability insurance policies are constructed in the same way as all insurance. They can be limited and specified with different terms, premiums, and excesses.

2.10.3. Incoterms 2000

Incoterms or international commercial terms were issued by the International Chamber of Commerce, ICC, and are a series of international sales terms that divide transaction costs and responsibilities between buyers and sellers in relation to transport. Incoterms also are closely related to the United Nations Convention on Contracts for the International Sale of Goods. ICC introduced the first version of Incoterms in 1936 and has updated it six times. The current version is valid from 1 January 2000 and is called Incoterms 2000. This includes rules about who pays for the freight (consignor or consignee), goods owner’s insurance, and special customs requirements, and also governs the liability and compensation from actors in the transport chain. According to Stöth (2004), the operator that commissioned the transport is responsible, but only for the part that pays the freight service. The four groups of delivery specified in the Incoterms 2000 are (Lumsden, 2006; Stöth, 2004):

• **Group C** – (i.e., CFR, CIF, etc.): The consignor purchases the transport but is not responsible for damages or losses until the first transport operator has taken possession of the goods. According to the terms of the CIP (carriage and insurance paid, valid for all transport modes) and CIF (cost, insurance, and freight, valid for sea transport modes), the consignor also must sign insurance in the name of the consignee.

• **Group D** – (i.e., DDU, DDP, etc.): The consignor purchases transport and stands for the possible risks until the goods are delivered. The most frequent terms are the DDU (delivery duty unpaid) and the DDP (delivery duty paid). The only difference between these is whether customs costs are going to be paid by the consignor.

• **Group E** – ExWorks: The consignee is responsible for booking transport, taking care of customs requirements, insurance, etc. The consignor only makes the goods available on the loading platform.

• **Group F** – (FCA, FAS, FOB): The consignor leaves the goods with a transport operator that has an agreement with the consignee. Different terms are used in this group: FCA, free carrier; FAS, free along shipment; and FOB, free on board). The most common is FCA, stat-
ing the risk transition from consignor to consignee as the goods are left to the first transport operator.

The usage of Incoterms 2000 is closely linked to the practical business relationship found in freights. Several authors (Agrell et al., 2004; Sheu et al., 2006; Closs et al., 2004; Manuj et al., 2008; Rice et al., 2005; Lee et al., 2003; Gaudenzi, 2006; Faisal et al., 2006 – a; Faisal et al., 2006 – b; Khan et al., 2007; Williams et al., 2008; and Ritchie et al., 2007) do not mention Incoterms as always present in business contact, including transport activities. Logistics research, by focusing on the use of risk management tools in supply chain operations, has forgotten the traditional method to govern transport related business risks. Figure 16 shows the rules in Incoterms 2000.

Figure 16: The division of risk from consignor to consignee by Incoterms 2000

The use of Incoterms 2000 in logistics operations needs more research to be better understood and put to more effective use (total supply chain cost meaning) in the future (Chapter 7.2).
2.11. Criminology and logistics

Sutherland, Cessey & Luckenbill (1992) define the scientific field of criminology as, “the body of knowledge regarding crime and delinquency as social phenomena. It includes within its scope the processes of making laws, breaking laws and reaction to the breaking of the law”.

If criminology is the scientific study of crime, then it must always begin and end with a discussion of the term crime. Laws must exist in order to break if the action is to be considered a crime, according to the principle “no crime without a law” or “nullum crimen sine lege.” This is the principle of legality, which is the centre of research in criminology (Sarnecki, 2003). This principle is decisive for this thesis.

2.11.1. The two different outlooks on mankind in criminology

It is possible to separate mankind into two different categories, depending on how decisions are made. This separation is a theoretical construction and its validity varies for every person in every situation.

Modern criminology uses rational choice theory as the basis for research. Rational choice theory, also known as rational action theory, is a framework for describing and modeling social and economic behaviour. This theory originates in the idea of the economic man in economic research, primarily microeconomics. This theoretical model is also central in modern political science and scientific fields such as sociology and philosophy. Rational choice theory assumes that individuals choose the best action according to the constraints, opportunities, functions, and abilities they face. Today, rational choice theory in microeconomics is defined best with the first four principles of microeconomics (Mankiw, 1997; Chapter 2.2.1). In short, the theory states that every presumed criminal is should be considered a rational person who makes decisions about potential crime from relationships between the benefits of the crime and the troubles and risk it brings. By increasing the perceived trouble and/or risk, it is possible to reduce criminal activity with this perspective (Sarnecki, 2003).

The opposite of rational choice is determinism. The idea is that the course of events depends completely on existing conditions. This approach refuses the idea of free will—everything is predetermined. In reality, every individual is a mixture of their ability to be influenced and the lawful. Among social scientists today, the idea of restricted free will is a common and useful insight. The cause of these restrictions can be found in the individual biological or psychological vulnerability, way of life, upbringing, social group, ethnic background, or society in which the individual lives, and how this affects his or her life with regard to their ethnic background, gender, and social position (Sarnecki, 2003).

These opposing perspectives of the human being as either the master of his own life or as a victim of circumstance can be found in every aspect of criminology. This contrast affects not only how we see the causes of criminal behaviour, but is also important with respect to the social response to criminal behaviour (Sarnecki, 2003). According to Bergman (2007), the current approach toward crime, punishment, and pardon is a good way to understand the surrounding society. It is commonly agreed that different crimes demand various mixtures of rational choice and determinism from the perpetrator’s side, where crimes of passion (sexual
crime, etc.) are considered more deterministic than property crimes (economic crime, etc.), which are more rational. That being said, the big difference appears when discussing the possible punishment for a certain crime. If an individual is responsible for his or her actions (rational choice), then the possible punishment will deter the crime; however, if the individual is a victim of circumstance (determinism), then it is useless to punish the individual. Therefore all crime prevention methods assume that an individual is responsible for his own actions and that he can perceive the consequences of those actions. The big question for the rational choice perspective is how each individual estimates the risk in a rational way. An individual that has received a formal or perceived punishment for an action previously should be less likely to commit that action again. The outcome of a formal punishment on the perception of risk is mixed (Horney, et al., 1992) and each individual should be considered not rational, but to act rationally on the margin.

2.11.2. Criminal prosecution and punishment

This discussion of the two outlooks on mankind in criminology clearly demonstrates the need to add theories from criminology into logistics. Several logistics authors claim that the weak prosecution of criminals is one reason behind the increasing need for security (Anderson, 2007; Badolato, 2000; Tarnef, 2006). In the context of the two outlooks on mankind in criminology, Anderson (2007), Badolato (2000), and Tarnef (2006), state the threats against logistics activities is simply based on the rational choice theory, while authors in criminology (Clarke et al., 2003; Felson et al., 1998; Horney et al., 1992; Klemke, 1992; Lab, 2000; Sarnecki, 2003; Speed, 2003) refer to an individual acting rationally on the margin which eliminates the deterring effect of potential punishment that Anderson (2007), Badolato (2000) and Tarnef (2006) suggest. The deterrent effect that a punishment can have on a perpetrator not to commit a certain crime is very low, due to that the perpetrators do not plan to get captured. Therefore has the risk for detection a bigger deterrent effect that the potential punishment (cf. Ekwall 2009 – b). The authors’ (Anderson, 2007; Badolato, 2000; Tarnef, 2006) request for stronger prosecution of criminals can be seen as a way to understand the surrounding society in general (cf. Bergman, 2007). Compare that to Williams et al. (2006) who state that risk management and TQM systems are normally linked to a punishment and reward system for the users. The difference between legal prosecution achieved by a state and a punishment and reward system controlled by a company or similar organisation is that legal prosecution involves a weaker relationship between action and consequence for the perpetrator.

Now suppose that a perpetrator acts fully according to the rational choice theory (only possible in theory)—from the perpetrator’s perspective, the risk of the crime prosecution while the opportunity is to get away it and gain something from it (depending on the uniqueness in perpetrator-driven forces). The risk side can be described simply as the risk of detection and the lawful punishment. The overall likelihood for a crime to be solved in Sweden was 16 percent of all reported crimes in 2007 (BRÅ, 2007). This percentage varies from one type of crime to another. The highest percentage of solved crime was homicide with 87 percent. For theft/pilfering from vehicle, the percentage of crimes solved is 4 percent, while the percentage of robbery (general) solved was 34 percent. These figures clearly demonstrate theoretically that an increase in the lawful punishment of a murderer presumably has a higher deterrent effect than for theft/pilfering from a vehicle (cf. Wang, 2000). This theoretical discussion presupposes that the perpetrators act solely according to rational choice theory. In reality, different strains of determinism will show the reasoning in this paragraph is fragmentary, but the logical thinking clearly limits the demand and clamour (from representatives of business and scholars) for more severe punishment to deter antagonistic threats against the transport network.
2.11.3. Opportunity to crime

Crime opportunity is a cornerstone of criminal behaviour. There are ten crime opportunity principles as follows (Felson et al., 1998):

1. Opportunity plays a role in causing all crimes,
2. Crime opportunities are highly specific,
3. Crime opportunities are concentrated in time and place,
4. Crime opportunities depend on everyday movements,
5. One crime produces opportunities for another,
6. Some products offer more tempting crime opportunities,
7. Social and technological changes produce new crime opportunities,
8. Opportunities for crime can be reduced,
9. Reducing opportunities does not usually displace crime,
10. Focused opportunity reduction can produce wider declines in crime.

Some of these principles are self-explanatory and easy to understand. All of them are valid for every type of crime and therefore they are also valid for crimes committed against the transport network. The more interesting examples of these opportunities will be explained and described later in this thesis. The most important thing to remember about crime opportunity is that an opportunity alone does not explain why a crime occurs because a crime needs a motivated perpetrator and opportunity to occur (Clarke et al., 2003). The theory of crime opportunity also refers to the fourth principle of microeconomics (Mankiw, 1997) - people respond to incentives - and there the degree of necessary opportunity or incentive depends on the individual. The incentives could range from vindication to morality, ethics, altruism, or determinism. This is the practical way the central principle in microeconomics, that all households and firms optimize, works (Chapter 1.1).

2.11.4. Routine activity perspective

The fourth of the ten crime opportunity principles states that “Crime opportunities depend on everyday movements” (Felson et al., 1998). Restated, crime opportunities depend on routines or predictability within certain boundaries. This statement also includes more principles than the original, implying that system predictability or routine provides crime opportunities. This is the routine activity perspective in criminology (Cohen et al., 1979). This theory provides a strong theoretical foundation for understanding crime and opportunities for crime. The routine activities perspective argues that normal movement and other routine activities play a significant role in potential crime (Roncek et al., 1991; Mustaine et al., 1998; Smith et al., 2000; and Sherman et al., 1989). The routine activity theory states that potential perpetrators may seek locations where their victims or targets are numerous, available, convenient, and/or vulnerable. Felson (1987) uses the illustration of “how lions look for deer near their watering hole” to explain the practical relevance of the routine activity perspective. According to Smith et al. (2000), social disorganization in combination with the routine activity theory can provide a wider and better explanation of property crime.

The transport network is made up of three levels (see chapters 2.4 and 2.8.3), infrastructure and the flow or movement of resources and goods. In the short time perspective, the infrastructure is fixed or completely predictable. The movement of resources between terminals, factories, and other nodes also is predictable to a large extent. The routine activity perspective states that predictability in infrastructure and resource movement will significantly contribute
establishing crime opportunities. The flow of material varies to a higher extent but depends on the actors within the supply chain. Therefore it is possible to predict the flow of goods to some extent. The routine activity perspective provides a theoretical foundation regarding antagonistic activities against the transport network (see Table 1). Thus, when the transport network changes, so does the theft opportunity.

### 2.11.5. Perpetrator’s decision factors

According to Smith (1776), human motives often can be described as driven by selfishness and greed. A perpetrator’s decision process can be described using five areas or components (Beck, 2002): temptation, motivation, opportunity, risk, and consequences. Each factor can have a negative or positive effect on the risk of crime and they can work in isolation or in combination depending upon the circumstances (Beck, 2002). The two sides (negative or positive effect) of each component are the key understanding of Smith’s belief (1776) that regardless of the motives, society as a whole can benefit if the different motives are exposed to the forces of a free market (Chapter 1.1). The five different areas or components of a perpetrator’s decision process can be described as the following (Beck, 2002):

**Temptation** is primary triggered by the perpetrator’s greed or need (even perceived need) (Beck, 2002). In a store, temptation is used to market a product, but during transport it is not. In stores, the staff handles large amounts of cash which is a possible means of temptation to the individual employee.

**Motivation** is an important factor in affecting the likelihood to offend. There are three parts which need to be considered: acceptability, neutralisation (or excuses), and marginalisation (Beck, 2002). Acceptability means what is accepted in the organisation and what is not. In this part of an offender’s motivation is the management’s model and actions which show which behaviour is acceptable. Neutralisation is used by offenders when the theft of money or goods is considered to be victimless and nobody really suffers. The third part of the motivation is marginalisation, which explains why some in the staff becomes dishonest. In general terms this can be described as the less the offender has to lose, the greater the risk for dishonest behaviour (Beck, 2002). Simply expressed, each individual’s morality can be used as a barrier against motivation for criminal acts as well as other legal but unwanted actions.

**Opportunity** is of critical importance and is based upon three significant factors: space, time, and position (Beck, 2002). Space refers to the place (where) for the opportunity while the time factor addresses when. The position factor refers to the work descriptions or tasks that provide crime opportunities.

**Risks and consequences** are the concern about the risk for discovery and the consequence of the crime. If the perpetrator perceived the likelihood of being caught as low or if the punishment is perceived as soft, then this may encourage theft.

The usage of these factors is based on the rational choice perspective of the perpetrator, or at least a bounded rationality. These five components of a perpetrator’s decision process can be summarised by the central principle in microeconomics that all households and firms optimize - “They do the best they can given their objectives and the constraints they face” (Chapter 1.1). The optimize principle is a risk assessment process based on the bounded rationality of the parties involved to optimize their gain (profit)/trouble (cost) equation from their point of view. The terms profit and cost are not used because the general principle only applies to eco-
nomically driven perpetrators; bounded rationality can be expressed with profit and cost, but profit or cost may not be possible to render in monetary terms, rather in perpetrator value terms.

2.11.6. Situation crime prevention

The development of situational crime prevention began in the early 1980s. The aim was to reduce factors specific to different types of crimes, locations, and situations. Situational crime prevention is based on the theoretical premise of rational choice (Clarke et al., 1985). Therefore the key factor in situational crime prevention recognition is that a crime often reflects the risk, effort, and payoff as assessed by the perpetrator (Clarke, 1995). These include the effort involved, potential payoff, degree of peer support for the action, the risk of apprehension and punishment, and individual needs (Repetto, 1974). The theory does not state that a perpetrator will commit a crime every time an opportunity occurs, but instead the potential perpetrator makes a calculated decision about the opportunity to commit a crime (Lab, 2000). In short, a perpetrator acts according to rational choice theory, seeking to maximize his utility with regard to a particular time and available resources (Bodman et al., 1997).

Some of the criticism against situational crime prevention states that this method leads to property crime receiving more attention than appropriate. Furthermore, situational crime prevention addresses the symptom and not the cause of the crime. This can lead to an excessive trust in technology (Crawford, 1998). Since cargo theft is a property crime, situational crime prevention is a useful method to address this problem. Basically this is achieved by applying the following three prevention principles (Clarke, 1992):

*Increased perceived effort* (Clarke et al., 1997) – Motivation to commit a theft is reduced if the perpetrator believes the crime is too hard to commit. Preventive actions based on this idea can be categorized as physical separation of the potential perpetrator and the object of the theft. This can be accomplished through the use of access control and physical barriers (fences, locks, etc.).

*Increased perceived risks* (Clarke, 1992) – If perpetrators think they will get away with a theft, it is more likely they will commit it. By increasing the risk for perpetrators they are less likely to commit a theft. This can be accomplished with surveillance systems, security personnel, and by increasing employee’s security awareness.

*Reducing anticipated rewards* (Clarke, 1992) – People are more likely to commit a theft if they can benefit from it. By making the target for the theft worthless or reducing its resale value it becomes less attractive for potential perpetrators. This can be accomplished by marking the goods with unique numbers or a product destruction device. Good examples of this principle are the safety cases used in transports of valuables and money and the ink tags used in fashion stores.

In 1997 Clarke and Homel added a fourth preventive principle based on rational choice theory (Clarke et al., 1997):

*Inducing guilt or shame* – A theft is more likely to occur if it can be excused by appeal to reasons such as “the company can afford it” or “I’ve worked hard for the company but they have not thanked me for it” (Tyska et al., 1983). This is a form of ethic relativity. Companies and organizations can affect this ethic relativity by using company rules, signs, and regulations
that demonstrate the right moral values. When theft is seen as an additional wage benefit for employees, this preventive action has failed (Muir, 1996). By appealing to people’s morals and making it easy for them to do the right thing, it will be more difficult to make excuses (Clarke et al., 1997).

2.11.7. Crime displacement

The theory of crime displacement says that crime prevention in one area may have unintentional consequences in other areas or situations. Therefore, crime prevention may not lead to an absolute reduction in crime. The theory of crime displacement is based on rational choice theory, with the following three assumptions about the potential perpetrator and target (Lab, 2000):

Crime displacement assumes that crime is inelastic (Reppetto, 1976) - This assumption indicates that the demand for crime is unaffected by preventive efforts. This is not true because all crimes are more or less elastic (Hesseling, 1994). Professional criminals are more inelastic while opportunistic criminals are more elastic (Reppetto, 1976).

The perpetrator has mobility (Reppetto, 1976) - Perpetrators have flexibility relative to time, place, method, and type of crime. In reality, perpetrators are limited in their mobility, adaptability, and flexibility relative to a particular crime, place, time, and method (Hesseling, 1994).

There exist unlimited numbers of alternative targets (Clarke et al., 1985) - The perpetrators have unlimited numbers and types of potential targets to choose from. In reality, the number of targets is limited in one way or another (Hesseling, 1994).

The theory of crime displacement states that rational thinking perpetrators with crime mobility will alter their behaviour in response to crime prevention efforts (Lab, 2000). Crime displacement will only occur when the alternative crime has a similar cost-benefit structure rationalised within the perpetrator’s decision process (Clarke et al., 1990). Based on the ten principles of theft opportunities presented earlier in this thesis and the configuration of the transport network, it is obvious that all opportunities cannot be eliminated, but they can be reduced by applying substantive preventive countermeasures. The object is to reduce crime opportunities which will lead to a change in potential theft situations. Therefore crime displacement is a valid theory (Reppetto, 1976).

Crime displacement can occur in several ways. Reppetto (1976) uses five types of displacement - crime, target, method, place, and time. Barr and Pease (1990) add another type of displacement, the perpetrator. The six types of displacement are explained below:

**Crime:** Transfer to other types of crime  
*Ex: offenders stop doing robberies and instead commit burglaries.*

**Target:** Transfer to other types of goods  
*Ex: offenders stop taking goods and instead target money transports.*

**Method:** Better locking devices force the offender to be more innovative  
*Ex: better doors force the offender to break-in through the windows.*

**Place:** Transfer to a less protected target in the same or other areas  
*Ex: if one area improves security then the offender attacks another area.*

**Time:** Transfer to different times of the day  
*Ex: better night security forces the offenders to strike during daytime.*
Perpetrator: Transfer to another perpetrator

Ex: Preventing one offender can create an opportunity for another offender.

The theory of crime displacement does not explain why perpetrators commit a certain crime or why some crimes are more attractive than others. Furthermore, it does not explain the perpetrator’s perceptions and reactions to changes in opportunities (Hesseling, 1994). Crime displacement is one probable explanation of why criminal patterns change in a certain system. A practical statement about crime displacement is that if perpetrators have the ability, mobility, and flexibility to exploit the weakest link in the chain, they will do so. It is the perpetrator’s ability to organize a successful crime and their relationship relative to the actors within the transport network that are the fundamental variables for categorizing perpetrators.

2.11.8. Professional vs. opportunistic perpetrators

Based on this fundamental categorization, there are two types of perpetrators: the professional and the opportunist (Klemke, 1992 - A). The professional perpetrator steals a certain product in exchange for money. He methodically plans the theft by identifying the weakest link in a security system (Weaver et al., 1985). The professional perpetrator is more concerned with the unpredictable elements in the security system (e.g., another human) than the technology. This depends on the perpetrator’s knowledge of the security system’s strengths and weaknesses. A professional perpetrator also can acquire the required technical expertise to overcome any predictable countermeasure (Kallis et al., 1985).

The opportunistic perpetrator steals an item because it is desirable or usable. This type of perpetrator does not steal for money. An opportunistic perpetrator acts on an impulsive decision-making process and does not plan the crime in advance (Klemke 1992, - B). There is little or no knowledge of a security system at any specific location. The presence of visible security measures instills fear in the potential opportunistic perpetrator (Beck, 2002).

However, both opportunistic and professional perpetrators try to optimise their behaviour in accordance with the central principle of microeconomics (Chapter 1.1) with the difference that they have different constraints (capability) to achieve their objectives.

2.11.9. Internal or external perpetrator

The position of the perpetrator relative to the company or organisation in which a crime is committed is of great importance for preventive and investigative purposes. Basically, perpetrators are either internal or external to the organization. An internal position (employment, previous employment, or similar relationship) brings access to transport information and increases the possibility of a successful crime. Transport information can be given to an external perpetrator by an employee. The external perpetrator also can retrieve the required information by hacking into the transport computer network or by employing non-criminal tactics such as tailing loaded lorries.

The greatest source of risk for businesses is trusted insiders (Barth et al., 1998). Some authors consider insiders to be involved in approximately 60 percent of all losses (Tryon et al., 1997; Robinson, 2009). Others claim there are no reliable figures (Muir, 1996). This is interesting when considering the fact that most countermeasures are implemented to reduce external theft (Beck, 2002). An internal perpetrator acts not randomly or in an unstructured way, but more as a response to social and environmental factors present in the work environment (Tryon et
According to Speed (2003), it is useful to divide employees into four different categories, depending on their duration of employment and age (Speed, 2003). This categorization can be used to separate potential dishonest employees and provide a degree of employee support and control (Speed, 2003). The best way to prevent an internal perpetrator is through the use of well thought out routines and procedures on how work should be accomplished (Muir, 1996). A graphical representation of the interplay between internal versus external and professional versus opportunist perpetrators is illustrated in Figure 17.

![Perpetrator's characteristics matrix](image)

**Figure 17: Perpetrator’s characteristics matrix**

The following are relative crime examples in Figure 17:

**A:** Shoplifter; walking past a parked, open, and unattended delivery lorry and stealing a package.

**B:** Organized theft without exact information; a pre-planned theft to steal from a parked lorry without knowing what it contains.

**C:** Organized theft with insider information; a pre-planned theft to steal from a parked lorry knowing what it contains.

**D:** Employees that commit a theft from their own company without any prior planning; a theft by a driver from his/her own lorry without prior planning.

The only common characteristic relative to all parts of the supply chain, including the transport network, is the perpetrator’s choice of if, when, where, and how to commit the cargo theft. Therefore, if a single part of the network implements countermeasures in an attempt to prevent crime, then the crime displacement theory predicts that criminal activities will move to another part of the network.
2.11.10. **Hot products**

The term hot products is commonly used in shrinkage management and its purpose is to point out a particular item or product as hot. These products are more likely to be stolen and therefore need greater attention in surveillance (Beck, 2003; Sherman et al., 1989). According to Clarke (1999), hot products are defined as products that are CRAVED: concealable, removable, available, valuable, enjoyable, and disposable. Which products are hot is often based on assumptions and opinions, but rarely by robustly derived data (Beck, 2003). By using accurate data factors such as opportunity and the black-market prospects, each item will be considered on equal basis as the pure value of the product (ECR, 2003).

2.12. **Logistics, risk management and criminology**

The three terms security, risk management, and crime prevention often are considered similar and always work together (Manunta, 1999; Borodzicz, 2005). This idea suggests that security and risk management are good from an ethics point of view because they reduce crime; therefore, more or better security or risk management will reduce crime. The problem here is that crime is defined by a law according to the principle “no crime without a law” (Sarnecki, 2003), while security or risk management has no philosophical attachment to law. Therefore, people on both sides of the law can have better security or risk management and that security and risk management are not necessary against crime.

Security for an individual or a group of individuals can, if unrestricted, jeopardise the security of others by threatening them or transferring threats to them. This type of discussion can be found with philosophers such as Hobbes and Mills. Unbounded or unrestricted individual security could threaten the authority of a state. This problem is demonstrated in the current debate about individual and private secure communication encryption, which some states want to make illegal unless they can break them. Taking this into account, a security problem may or may not be a legal problem. As a concept, security involves a protector or guardian and a threat against an asset or object (Borodzicz, 2005). This threat can be from either side of the law. To obtain the right security, it is vital to answer who is protecting what, from whom, in which situation, to what extent, and to what consequence (Manunta, 1999). As stated before in this thesis, security can be seen as contextual risk management (Chapter 2.9).

Contextual and statistical risk management approaches as crime prevention methods work in different ways and address different types of potential perpetrators. This demonstrates the difference in the philosophical views of contextual and statistical risk management. Statistical risk management needs a fairly predictable world, or at least a larger amount of trustworthy statistics. Since previous events or incidents are the basis of statistical risk management, it cannot deal effectively with a self-inflicted alteration of the threat pattern. Therefore, statistical risk management is effective in crime prevention if the potential perpetrators are limited to unsophisticated and indifferent methods based on opportunistic behaviour (Manunta, 2002). However, as potential perpetrators become more sophisticated and gain more capability, the accuracy of statistical prediction will reduce dramatically. Antagonistic perpetrators study the victim to discover routines and regularities and improve their skills with this knowledge (planning, technologies, and tactics) to maximize their likelihood for success (Clutterbuck, 1987). The prevention of antagonistic threats by following current business trends makes the system even more predictable. Military special forces and similar organizations have proven this time after time (Manunta, 2002).
2.12.1. The antagonistic threat triangle in logistics

The wicked problem of antagonistic threats against the transport network changes depending on the stakeholder that delivers the judgment and interpretation of the problem. Therefore, the necessary common ground for describing the problem is missing or described differently. According to Lawson (1997), social activity is embedded in material circumstances. This makes a separation of material and non-material structures of the logistics business impossible. As Aastrup and Halldórsson (2008) claim, the perception of social phenomena needs to be included in the analysis. A contextual understanding of the occurrence of antagonistic threats in freight processes is vital. This thesis uses several theoretical models to describe different aspects of logistics and antagonistic threats. All models provide with a different viewpoint and therefore contribute to the contextual understanding.

The limitations and demarcations in this thesis also limit the reliability of its results. Regardless of this fact, simplifications are a very powerful tool to present basic and advanced features/elements in a complex system. Insights from complexity theory guide the search for a few guiding principles that describe the behaviour of the system (Gault et al., 1996). To think in terms of complexity means to appreciate the idea that every change affects, in non-linear ways, other parts of the system. Complexity theory gives us a system understanding based on subjectivity and paradoxes instead of objectivity and rationality in interaction between actors (Macbeth, 2002).

The complex relationship between transports and antagonistic threats starts with the motivated perpetrator and continues with the logistics functions that relate to the perpetrator and elements of crime. This follows the definitions of antagonistic threats used in this thesis:

*Antagonistic threats are deliberate, illegal and hostile threat against the planned or desired logistics process, function, and structures.*

The three elements of crime clearly state the requirements for a crime - a perpetrator, an object, and lack of a capable guardian. Therefore, antagonistic threats also require similar elements of a perpetrator, an object and a lack of security. If one of these elements is missing then there is no antagonistic threat; it is the potential perpetrator that determines whether the object is desirable and if security is insufficient. The relationship between antagonistic threats, elements of crime, and three intersections is presented in Figure 18 and represents the antagonistic threat triangle in logistics. The antagonistic threat triangle is an illustration of the elements, events, and relationships within the supply chain risk context that explain and simplify the understanding of antagonistic threats.
The relationship between a potential perpetrator and supply chain security is referred to as the crime displacement effect. The supply chain internal control zone is limited to objects and security features. This means that supply chain performance will be determined by one of these two elements. The opportunity, found between the element’s potential perpetrator and object, is the third threat feature presented in the antagonistic threat triangle. Therefore, handling of an antagonistic threat against logistics is a balance between the desired supply chain performance and reducing opportunity while avoiding potential crime displacement.

2.13. Research questions – theoretical verification

The four research questions in this thesis are derived from the background description presented in Chapter 1.1. However, the theoretical validity of those questions needs to be verified by deriving the same research questions from the framework presented in Chapter 2.

RQ 1 What are the characteristics of antagonistic threats against the transport network?

Theories from the scientific field of criminology can be used with great advantage to describe the characteristics of antagonistic threats. The context of transport and theories from criminology shall cooperate to describe the characteristics. The validity of the research question is high due because the cause (potential motivated perpetrators) is the key to understanding and managing the risk of antagonistic threats and the description of the cause can only be achieved with theories from criminology. In addition, the first four principles of microeconomics can be used to illuminate the motives or driving forces behind perpetrator behaviour.
RQ 2  How are these antagonistic threats organised and managed today?

The existence and management of threats/risk in relationship to transport and supply chain management is as old as the need for transport itself. The pragmatic approach that has evolved throughout the centuries has focused on two things, namely cause and reducing the impact. The most developed pragmatic approach is reducing the impact through insurance and international regulations and convention that appoint liability and commitment from the actors in the business transaction. The actor with liability implements measures that reduce the cause. The usage of insurance policies is so well integrated and well functioning that it is virtually impossible to visualize a business world without insurance.

RQ 3  What are the effects on the transport network with both regard to the characteristics and the management of these antagonistic threats?

The relationship between the management and characteristics of antagonistic threats is dynamic, environmentally dependent, and always changing. Therefore, what works at one place/time may not work at another place/time and managing these antagonistic threats depends on the local environment. All actors managing the risk for their business within their own liability depend on the use of international regulations and conventions.

RQ 4  How can antagonistic threats be managed more effectively?

As presented in Chapter 1.6, this research question can be divided in three ways depending on the definition of more effective. Therefore, the theoretical verification uses the same three perspectives (cost, occurrence, and impact).

Cost for each stakeholder: Membership in a certain supply chain can, in practical terms, be reduced to the expression, “what’s in it for me?” This is a simplistic way to see the world, but sometimes simplistic expressions provide a good image of the reality stakeholders faces. Why stakeholders should be members of a certain supply chain is rarely addressed in supply chain theories. The most common idea in this direction is that each stakeholder gains more as a member than they do not being a member. Therefore it is possible to state that each member of a supply chain is a member because of the first six principles of microeconomics (Chapter 2.2.1), but it does not explain how each member maximizes their profit from being a member. It is in this perspective that the cost for antagonistic threats should be understood, because their occurrence and impact result in higher cost for the whole chain or a share of its members.

Cost for the total supply chain: In the total supply chain perspective, the total cost for managing the problem of antagonistic threats is only one special cost that needs to be managed effectively to reduce the cost for the whole supply chain. The problem linked to the occurrence of antagonistic threats from a cost share perspective is addressed in Paper B. Also, it is linked to the theoretical discussion of supply chain misalignment in order to master the dynamic in a supply chain with unnecessary vulnerability.

Occurrence: The occurrence of the problem of antagonistic threats against the transport network is linked to two different attributes from a theoretical perspective—predictability (the possibility of statistical forecasting the problem) and impact on supply chain performance. The first attribute is linked to the credibility of the statistical sources of information about
antagonistic threat history. This thesis refers to some of these statistical sources. The credibility of these sources is addressed in Chapter 3.6. The second attribute relates to the consequences following an antagonistic threat. Antagonistic threat consequence reduction is of vital importance, and support for this is found in vast amounts of the current SCM literature. The big difference is that current SCM literature addresses internal supply chain disturbance (bullwhip and domino effect), but while the antagonistic threat-generated disturbance may have similar effects, it functions in a different context that requires other reduction strategies.
3. Methodological framework

This chapter will describe the methodological aspirations for this thesis and will elaborate on the tools used in the processing and analysis of the data.

3.1. Research procedure

The research conducted in this thesis can be described as a step-by-step process. The framework of this thesis was developed as a result of empirical findings and theoretical insights. The research is characterised by continuous development and validation of the framework of this thesis. Validation was accomplished by presentations for and feedback from several experts in the field. This process was conducted several times. Therefore, it is difficult to state whether the theory or empirical data came first. In terms of theory of sciences, this research procedure is neither deductive nor inductive. Instead, the research procedure was governed by the need for a deeper and clearer understanding of the general problem of antagonistic threats in the transport network but also with a research question-centred view on what was important during the research process. Therefore, the research procedure can be categorized as abductive (Dubois et al., 2002; Kovacs et al., 2005). This thesis is written by using a deductive approach to develop a theory based on other theories and observation. The papers in this thesis should be viewed through the inductive method to prove the deductively developed theory (Kekäle, 2001). The deductive approach helps to substantiate the objectivity of the research (Popper, 1959).

According to Stock (1997), the use of theories from other scientific fields is common in logistic research. These theories derive from areas such as economics, philosophy, and organization theory. The interdisciplinary exchange of views, ideas, and theories is needed to develop as an applied science (Klaus et al., 1993). Stock (1997) points out three benefits from borrowing theories from other disciplines:

1. Learning from the experience of others,
2. Advance in knowledge and understanding, which might not have occurred otherwise, or perhaps taken longer, could occur more quickly,
3. The inclusion of theories from other disciplines further enhances the linkage between logistics and those disciplines.

In the paper, “Applying theories from other disciplines to logistics,” Stock (1997) illustrated his view by discussing several past areas of interdisciplinary research in logistics. One exchange area that he does not address explicitly is the one used in this thesis, logistics and criminology interaction. Also, Stock concludes that logistics will continue to borrow theories and ideas from other disciplines as it develops as a scientific field. This thesis confirms Stock’s conclusion.

3.2. System approach

The research in this thesis follows the tradition in logistics of using a system approach to answer research questions (Aastrup et al., 2008; Hellström, 2007; Gammelgaard, 1997; Gammelgaard, 2004). Checkland (1999) describes the concept of system as: “The central concept ‘system’ embodies the idea of a set of elements connected together which form a whole, this...
showing property which are properties of the whole, rather than properties of its components”. The main idea of system theory is to illuminate holistic thinking; it is based on the assumption that a whole system is different from the sum of its components (Churchman, 1968; Von Bertalanffy, 1969; Hellström, 2007). According to Hellström (2007), one of the main issues in system theory is how elements interact with each other in the system. Forrester (1961) remarked that events in one part of the material flow affect other parts of the flow. The “total systems perspective” is the foundation for the logistics discipline to include the entire material flow in research (Gomes et al., 1988). According to Checkland (1999), there are two types of system approaches - hard and soft system thinking. The hard approach is related strongly to the use of mathematical models and simulations while the soft approach focuses on solving problems by involving and interacting with people. The traditional hard system approach implies both an objective reality and a top-down perspective on the system.

The system approach in this thesis is more of a soft-system thinking where reality is described in subjective terms and the whole system has the distinctive trait of vague or undefined boundaries between system components and the surrounding environment. Therefore, this thesis uses a complex system approach in which paradoxes and bounded rationality describe the system’s behaviour. This simplification is done with the purpose of illuminating the wicked problem of antagonistic threats. The ultimate customer (cf. Christopher, 2005) for the antagonistic threats is the black market for economic threats or if mixed with legal products, the grey market. For non-economic threats, the ultimate customers are more difficult to establish because the wanted effect/consequence has weak and indirect links to the actual event.

The system approach allows logistics to be seen as more than the sum of its activities. There are two attributes that distinguish a system: its boundaries and the context in which is presented (Wilson, 1990). The models and theories from supply chain management and logistics used in this thesis do not have legal aspects, but it is implied that they are developed from and for the legal logistics system as they are presented by their authors. This does not make them invalid for analysing the occurrence of antagonistic threats against logistics operations; instead it illuminates a research gap. The theories from supply chain management and logistics are valid on both sides of the law if taking into account the divergence that depends on the legal boundary. The explanation is found in the context of supply chain management, where the ultimate customer’s demand is the goal for the stakeholders regardless of the legality of the processes and products involved (cf. Christopher, 2005). Therefore, legal and illegal supply chains aim to fulfil the ultimate customer’s needs, with regard to product, price, and place.

The majority of complex systems indicate a large amount of redundancy. By using this redundancy, it is possible to simplify the system and gain understanding and the ability to control it (Waidringer, 2001). This thesis defines the legal descriptions and criminal threats against and within supply chain management activities that make up the systems context and boundaries. This context difference affects the configuration of the supply chain system in a way in which the same variable will receive different importance. The main idea behind a system approach is to understand not only the components or parts of the system but to understand their interaction in their natural environment. According to Arbnor and Bjerke (1997), the system-theoretical approach can be divided into three parts:

- System analysis: The researcher creates a model of a real system to identify internal and external factors that affect the system.
- System construction: The researcher creates an imagined system into a system model.
• System theory: The system model and its factors are validated by more than one real case. System analysis and construction are part of the development process for system theory.

The system theory used in this thesis follows Arbnor and Bjerke’s approach. First a model system is created and defined by identifying internal and external factors (Chapter 1). Secondly, an imagined system is created (Chapter 2) within the boundaries of the system model. Then, the complexity of these two systems was reduced by the removal of redundancy in each model (Figure 3). The last step is to describe the interaction between the elements of the model and locate this model in the supply chain structure that contains the ultimate customer involvement in form of black, white, and grey market demands (see chapters 4-7).

3.3. Complexity theory

The principles of complexity theory suggest that physical, social, and mental worlds are non-linear and complex. The perception of supply networks and logistics as complex is emphasized by several authors (Bowersox et al., 2002; Christopher, 1998; Cox, 1999; Lambert et al., 1998; Lumsdén et al., 1998; Tan, 2001; Borodzicz, 2005 Gallagher et al., 1999; Mainzer, 1997). Milgate (2001) observes that, “complexity should be viewed as a deterministic component more related to the numerousness and variety in the system” i.e., logistics systems could and should be reduced heavily and simplified. There are several others proclaiming the same simple approach to deal with logistics complexity (Childerhouse and Towill, 2003a, 2003b; Narasimhan and Jayaram, 1998; Towill, 1999; Towill, Childerhouse and Disney, 2000; and Wilding, 1998). However, Choi, Dooley and Rungtusanatham (2001), Johannessen & Solem (2002), and Nilsson (2005) question these simplified and reductionist approaches. They believe, instead, that “logistics processes, where human beings are involved, are not simply a sequence of mechanical devices which can be assumed to work along positivistic beliefs, but instead a complex network of living, innovative, creative, and evolving creatures which react and adapt dynamically to their perceived environment, and try to proactively create what they themselves, or collectively with others, find to be beneficial for their own interests” (Nilsson, 2005). With such a perspective on logistics, the reality of transport issues can be examined and empirically identifiable actions such as minimizing personal losses, wishes for blurry borders, keeping out of trouble, etc., can be better understood.

Insights from complexity theory guide the search for guiding principles that describe the behaviour of the system (Gault et al., 1996; Gallagher et al., 1999; cf. Keynes, 1936). To think in terms of complexity means to appreciate the idea that every change affects, in non-linear ways, other parts of the system. Complexity theory gives us a system understanding based on subjectivity and paradoxes instead of objectivity and rationality in interaction between actors (Macbeth, 2002; Mainzer, 1997).

Complexity is closely related to uncertainty, because the underlying principles of determinism and predictability are desired for business. Certainty in business means that every factor is fully deterministic and the outcome will be fulfilled in a precise manner. However, uncertainty is simply a key characteristic of any economic activity (von Oetinger, 2004) and with uncertainty comes risks. A major consequence of uncertainty in business is that each actor, as rationally as it can from its subjective perspective, tries to control and reduce its uncertainties.

While knowing and predicting what customers want often involves a great amount of uncertainty, it is only one of many questions to be answered. Also, each manager needs to answer
the question as to when, how, and why the customer wants a certain product and how it is possible to get it to the customer; i.e., logistics uncertainties. According to Nilsson (2006), logistics uncertainty can be grouped into four different dimensions:

1. Customer’s demand and expectations
2. Internal processes
3. Human factors
4. General trends

All four dimensions of logistics uncertainty will, to varying degrees, occur throughout the transport network. This indicates that the complexity within the transport network increases due to uncertainty in different dimensions. According to Nilsson (2006), the message in logistics literature is that the treatment for uncertainty is to reduce it as much as possible. This is also, as mentioned above, the valid view on complexity. The actors within the transport network handle its complexity in similar ways - the actors are, to varying degrees, involved in activities that aim to reduce or limit their own complexity and that of the transport network. The more complexity in the transport network, the more complexity is transformed through it. This increases the need for handling strategies that reduce the effects of complexity.

3.4. Research process

The research process began with a literature review of previous research in the field and related scientific fields to get a deeper understanding of the subject and generate ideas for the research presented in this thesis. A methodological strategy was formed based on the literature study. This strategy can be described as an abductive approach with a focus on understanding the business itself, the problem of antagonistic threats against the business, and the interaction between the logistics business and antagonistic threats. This research strategy was chosen because of the wicked problem description, where contextual understanding is essential to understanding the problem.

The research in this thesis is based on eight studies conducted during a five-year period. They can be categorized according to the general purpose of the research. These categories are exploratory, descriptive, and explanatory. According to Yin (1994), each research category has different methods, i.e., where an exploratory study uses case studies, a descriptive study uses the survey approach, and the explanatory study uses an experimental approach. Yin argues that these types of methods are not locked into one particular category of research, but can all be used to strengthen each other and in different combinations. This multiplicity research approach follows the trend within logistics research (Näslund, 2002; Gammelgaard, 2004; Kovács et al., 2007). Several of the papers appended to this thesis (B, D, and E) use cases to support the results. This fulfils Ellram’s statement (1996) that “case studies are excellent for theory building, for providing detailed explanations of ‘best practices,’ and providing more understanding of data gathered”

The research process started with an exploratory study. The intention was that the outcome of the study would form a more precise problem definition (Hellevik, 1984). This study formed a new and more precise research question that gave directions for three more exploratory and descriptive studies. Table 15 illustrates the research strategies used in studies related to this thesis.
<table>
<thead>
<tr>
<th>Paper</th>
<th>Exploratory</th>
<th>Descriptive</th>
<th>Explanatory</th>
<th>Normative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper A</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Paper B</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Paper C</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Paper D</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Paper E</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper F</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Paper G</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Paper H</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Table 15: Classification of the appended papers

The main reason for the use of this process was the lack of reliable information, both primary and secondary, that otherwise would have been a bigger problem.

During the research process, the reliability of the information about criminal activities against logistics has been an issue for the following reasons:

- Companies are reluctant to state in official information channels that they have problems with criminality. This is for business reasons such as imagined “bad will” from potential customers.
- The growing use of company boundaries and insurance companies to limit the economic consequence of an incident has reduced the companies’ willingness to address the actual problem instead of its economic effect.
- The lack or imagined lack of interest in this problem from the legal system has contributed to the reduction of willingness to report crimes to the police.
- In all criminal statistics there is a large amount of hidden statistics, which reduces the reliability of these sources.
- The difficulty to establish the exact procedure (location, modus, etc.) of an incident.

Together these questions regarding the reliability of information about criminal activity indicate that a qualitative approach is necessary to get a better understanding of the problem of antagonistic threats against cargo flows.

Business involvement in this thesis has been affected, to varying degrees, by these five reasons for reliability of information about criminal activities. Therefore, companies and organisations have been granted anonymity in their contribution to the research and results in this thesis. The companies and organisations that were involved more than once or in any of the eight papers presented in this thesis are mentioned in Appendix B.

3.4.1. Research chronology

The research in this thesis is the result of several years of work. The studies that constitute this thesis are referred to in this chapter according the paper in which the results are presented. The years 2003 and 2004 were filled with information checks, literature surveys, and building the empirical network for this topic. Three studies were started in 2005 (Papers A, D, E). An earlier version of Paper A was presented at a business conference, and in 2006 the researcher presented the report that provides the practical background for Paper D (Dillèn et al., 2006). Also in 2006, the researcher wrote the licentiate thesis which contained earlier versions of papers A, D, E and the raw data for paper C. The thesis was presented in early 2007.
Meanwhile the licentiate was written and the ideas for papers B and F emerged. In 2007, these studies were accomplished. During the analysis phase of the empirical data for Paper F it became evident that this data needed to be analysed from more than one perspective. Therefore this data was used in two papers (F, G). The two perspectives in these papers clearly demonstrate the need for a multi-approach methodology in this topic. Writing this thesis started in late 2007, along with finalisation of the appended papers.

The idea for Paper H was raised from work on papers A and C. This process is presented in Figure 19, which also shows relationships between the studies. A direct influence is demonstrated by a continuous line while indirect influence is illustrated with a dashed line.

![Figure 19: Research chronology](image)

Naturally is it difficult to pin-point the influence between the papers because the work with several of them was done simultaneously and they influenced each other. Figure 19 illustrates the major influences.

### 3.5. Literature review to find the research gap

The research with regard to risks in a supply chain is fairly new and it started with risks and purchase (Khan, 2007). Since then several authors have addressed the relationship between risk and supply chains (Robinson et al., 1967; Williamson, 1975, 1979; Burnes et al., 1998; Burnes et al., 1996; Womack et al., 1990; Cousins et al., 2004; Hood et al., 2005; March et al., 1987; and Kraljic, 1983;). Studies of supply chain risks seldom address the causes of risk (Christopher et al., 2004 - a, 2004 - b; Juttner, 2005; and Sheffi, 2001). They simply mention supply chain risk sources without discussing causes such as theft, smuggling, sabotage, and criminal activity other than terrorism.

“Risk and supply chain management: creating a research agenda” by Khan and Bernard (2007) contains a good review of the current research on supply chain risk management. The only criminal offense mentioned in this paper is terrorism. Therefore, this paper follows the tradition of other supply chain risk papers (Christopher et al., 2004 - a, 2004 - b; Juttner,
The reason for this may be found in Chapter 1.1.7 where the FFL statistics clearly state that cargo damages are responsible for approximately 90 percent of all claims on LSP liability. This shall be compared to the data in Chapter 1.1.6 that states that loss (regardless of the cause) is lower in distribution than in the manufacturing and retailing steps in a general supply chain. Therefore, the main reason for loss in a supply chain is not the result of antagonistic threats but instead is due to process failures or other unwanted but legal incidents. Regardless of this fact, solutions and management strategies can address and influence the occurrence and cost structure for antagonistic threats and process failures.

The reasons behind mentioning terrorism in several supply chain risk papers maybe threefold. First, Sheffi (2001) points out the effects of the World Trade Center terrorist attacks on the global flow of goods. The effect maybe indirect but were devastating nevertheless. This event and non-antagonistic events such as Hurricane Katrina and other natural disasters demonstrated the power to disrupt or cause uncertainty in supply chains (Elliott, 2005; Peck et al., 2002). Secondly, terrorism fund raising through criminal activities (Hardouin et al., 2006), means all terrorism is an antagonistic threat. Third, the tools and strategies for handling antagonistic threats are partly governmental (police and justice system) and partly consequence handling (insurance business and conventions). The occurrence of terrorism in the world is presented in Chapter 1.1.5. The statistics show that it is difficult to understand the attention the attacks have gained in comparison to other antagonistic threats (see chapters 1.1.3, 1.1.4, 1.1.8, and 1.1.9). The explanation for this may be the difference in risk apprehension between individuals and risk aversion—that a larger impact is considered more serious than a higher likelihood for the same risk cost (De Becker, 2002; Sjöberg, 2000; Bernstein, 1996; Ekenberg et al., 2001).

Regardless of why criminal activity (except terrorism) was not included in general threats against the supply chain, the criminal problems are there (Chapter 1.1) and they need to be understood. The three elements of crime are equally good to describe terrorism and other crimes. The key difference is the motivated perpetrator’s decision process and the desired outcome.

This thesis is a first attempt to bridge this gap in the logistics research.

3.6. Data sources and their reliability

The validity and credibility of the research depends on the use of data and the sources of this data. The data sources are normally divided into primary and secondary sources. The primary sources are interviews and the secondary sources are literature, databases, and the Internet. Interviews can be executed in several different ways. The manner the researcher chooses to conduct the measurement and data collection depends on the aim and purpose of the research. In this thesis, the scope was to understand and demonstrate the antagonistic gateways between the legal and illegal logistics systems from a supply chain perspective.

The purpose of the primary data is to give a deeper understanding of the problem with antagonistic gateways in the transport network. Therefore the primary data is collected during interviews that involve few questions and focus on the description of the problem. Primary data is used in this thesis to bring understanding of the research questions.

Regarding secondary data, it is always important to ask where the data comes from and how it is collected and analysed. The main problem with secondary data is explained with the ques-
tion of where and when it was transformed from primary to secondary data. The difference can appear small, but when the data is used it can affect the entire study. The secondary data and information in this thesis are used only as trend indicators and not as a standalone answer to any research question.

The information about black logistics comes from official reports and interviews with security personnel or personnel with similar assignments. The black logistics description is based on secondary data instead of the preferred primary data because primary data is very hard to get. Valid statistics are difficult to obtain because often they are incomplete or limited in scope (Nowotny et al., 2002). Furthermore, official criminal statistics are questionable because they contain actual and unsubstantiated crimes but omit unreported actual crimes (Lab, 2000). The secondary data from reports was collected from trustworthy institutes such as the FBI, DEA, Europol, and the European Commission. In some cases the report came from a trade association, but this occurs only for counterfeited products.

### 3.7. Interviews

The interviews conducted for this thesis were made in the same way. Qualitative interviews are motivated by the fact that the issue of the study is sensitive, but have the same negative as ordinary survey questions have about thefts—the interviewees answer questions in a politically correct way, which makes the data less reliable (Seidman, 1998). The problem of correctness does not disappear during interviews, but it gives the opportunity to explain questions and to ask respondents to explain themselves. By doing so, the conversation became more relaxed and a sense of trust was established between the researcher and respondent that made it easier to go into more formal descriptions of highlighted security problems (Kvale, 1997).

All interviews were conducted as a conversation and all normative discussion was forbidden during the interview. The purpose was to get the interviewees to state their true opinion and experience. For the same reason the interviewees were guaranteed anonymity so they would not fear reprimand from their employers. The interviews all ended with a mutual survey of the notes taken to ensure they accurately represented the interview (Mishler, 1986).
3.8. **Empirical data used in the different papers**

The validity and credibility of the research depends on the use of data and the sources for this data. This leads to that both the amount and quality of the different empirical data sources are vital for the credibility of this thesis. In table 16 are the different types of empirical data presented.

<table>
<thead>
<tr>
<th></th>
<th>Official statistics sources used</th>
<th>Survey</th>
<th>Interviews</th>
<th>Case studies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper A</td>
<td>5</td>
<td>4 participants</td>
<td>6 interviews</td>
<td>-</td>
</tr>
<tr>
<td>Paper B</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>Paper C</td>
<td>-</td>
<td>30 participants</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Paper D</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>Paper E</td>
<td>9</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>Paper F</td>
<td>3</td>
<td>-</td>
<td>15 interviews</td>
<td>-</td>
</tr>
<tr>
<td>Paper G</td>
<td>4</td>
<td>-</td>
<td>15 interviews</td>
<td>-</td>
</tr>
<tr>
<td>Paper H</td>
<td>2</td>
<td>42 participants</td>
<td>3 interviews</td>
<td>-</td>
</tr>
</tbody>
</table>

*Table 16: Empirical data sources used in this thesis*

3.9. **Verification and validation of results**

Validity and reliability of the research are two factors that intend to verify the results of the research process and ensure the credibility of the research. Validity means that the methods chosen measure what is intended. The problem of achieving valid information or data appears less in qualitative methods or analysis than in quantitative methods, because qualitative methods give certain proximity to the researcher and subject. This proximity is not free from problems, because it means the researcher and subject influence each other. To avoid the interaction between researcher and subject, the researcher needs to be aware of how he or she affects the subject and take that into consideration during the research process (Holme et al., 1997).

Validity can be separated further into internal and external validity (Yin, 1994). Internal validity aims to establish a causal relationship to show that conditions lead to other conditions by pointing out the distinct relationship between them. External validity aims to establish a domain where the research results can be generalized. Internal validity is achieved with the theoretical framework and external validity is accomplished by the three papers that are part of this thesis.

The reliability of the research indicates how effectively the methods can resist chance. This problem is not as central in qualitative methods as in quantitative methods because qualitative methods are used to understand certain factors and courses of events. However, quantitative methods originate from statistics and therefore are more sensitive to random factors (Holme et al., 1997). A good way to achieve high reliability is to use obvious and clear questions. During an interview it is important to give the interviewee all the time he/she needs and to conduct the interview in an environment where the interviewee feels safe. The reliability of this research is achieved because all interviews were based on simple questions and conducted in a descriptive way. All interviews were done by the author.
4. Summary of appended papers

The theories presented in the framework in this thesis are used in one or more of the eight papers in different ways. The results of the eight studies conducted in relationship with this thesis are related to the four research questions presented in Table 17:

<table>
<thead>
<tr>
<th>Paper</th>
<th>RQ1</th>
<th>RQ2</th>
<th>RQ3</th>
<th>RQ4</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>F</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

*Table 17: Relationship between the papers and the research questions*

The eight papers address different aspects of the wicked problem of antagonistic threats against the transport network. Therefore, the competing interests and lack of a universal solution can be illuminated in several perspectives.

The authors’ different roles in the appended papers are described in Table 18.

<table>
<thead>
<tr>
<th>Paper</th>
<th>First author</th>
<th>Second author</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Daniel Ekwall</td>
<td>-</td>
<td>Sole author</td>
</tr>
<tr>
<td>B</td>
<td>Daniel Ekwall</td>
<td>Fredrik Nilsson</td>
<td>The study was designed and accomplished by E. with support from N. The paper was written by E. and N. contributed with complexity theory descriptions and analysis. The conceptual design was accomplished by N.</td>
</tr>
<tr>
<td>C</td>
<td>Daniel Ekwall</td>
<td>Kenth Lumsden</td>
<td>The study was designed and accomplished by E. with support from L. The paper was written by E. and L. contributed methodological and theoretical framework descriptions.</td>
</tr>
<tr>
<td>D</td>
<td>Daniel Ekwall</td>
<td>Håkan Torstensson</td>
<td>The study was designed and accomplished by E. with support from T. The paper was written by E. and T. contributed theoretical framework descriptions.</td>
</tr>
<tr>
<td>E</td>
<td>Daniel Ekwall</td>
<td>-</td>
<td>Sole author</td>
</tr>
<tr>
<td>F</td>
<td>Bertil Rolandsson</td>
<td>Daniel Ekwall</td>
<td>The study was designed and accomplished by both authors. The empirical material was collected jointly. Paper F was written from the perspective of social science while paper G uses the logistics perspective. This is the difference in author contribution.</td>
</tr>
<tr>
<td>G</td>
<td>Daniel Ekwall</td>
<td>Bertil Rolandsson</td>
<td>The study was designed and accomplished by M. with support from E. The paper was written by M. and E. together.</td>
</tr>
<tr>
<td>H</td>
<td>Arsham Mazeradi</td>
<td>Daniel Ekwall</td>
<td>The study was designed and accomplished by M. with support from E. The paper was written by M. and E. together.</td>
</tr>
</tbody>
</table>

*Table 18: Different authors’ roles in appended papers*
4.1. Link between appended papers

This thesis addresses antagonistic threats against the transport network. The eight appended papers illuminate several perspectives and this thesis uses all of these perspectives to provide a contextual understanding of the wicked problem. The relationship between the different papers and antagonist threats against the transport network is presented in Figure 20.

Paper A has two purposes in this thesis. The first is to illustrate the need for the use of criminology theories in logistics research, and the second is to provide an initial exploration of the problem with antagonistic gateways in the transport network. During the interviews conducted for Paper A, one of the interviewees said that “even the criminals need to transport their stolen goods from the point of theft to their customer”. This statement formed the research purpose of Paper E, to analyse the similarities and differences in the design of logistics systems with respect to the legality of transported goods. This means the legality of the goods is vital when it comes to taking goods from their point-of-origin to the customer. Paper E addresses the context of illegal actions in relation to logistics more than the direct threat against logistics performance. Papers B and C illuminate the consequences of antagonistic threats on the transport business.

The research conducted in Paper D was related to the need for and design of a secure parking space for road transport. This is linked to Paper A because more than one of the interviewees pointed out that parked lorries were a easy target for theft. Paper D answers the important question of why we need these parked lorries and how problems/risks/uncertainties can be reduced in the supply and transport chains. This paper is a continuation of a study presented in a report (Dillén et al., 2006). The main result of that report is that crime as theft of cargo and/or lorry has become a big problem because of the extended use of parking spaces for lorries during road transport. The extent of the problem varies throughout Europe. The study was limited to Sweden with a European outlook.

Paper D addresses the problem of antagonistic gateways from the transport network’s perspective and explains why certain network characteristics cannot be altered without changes in supply chain characteristics. It focuses on the supply chain’s need for temporary storage to function as a disturbance neutralizer and reduce risk and uncertainty from within the supply chain. However, temporary storage areas close to receiving terminals provide potential perpetrators with a recurring crime opportunity and are the weakest link in relative terms. Therefore, to reduce the total risk for the supply chain, it is necessary to reduce crime opportunity in the temporary storage area.
The conclusion in Paper D shall be compared with the findings in Paper E. Where Paper D states that the predictability of the transport network is vital for the legal supply chain, Paper E states that the predictability of the transport network can be abused for smuggling purposes. Paper E shows that the decisive difference between black and white logistics is found in information about the products, transport routes, ownership, and domestic laws. The need for correct information cannot be overestimated in terms of discovering illegal goods in legal logistics flows. The pure nature of illegal goods governs the choice of logistics setup, concealed shipment, or internal systems. The more difficult it is to establish whether a product is illegal or not, the more likely it is to be transported in the white logistics system. By using or stating reliable false information to the white logistics company, it is possible to increase the likelihood for the illegal shipment to reach its consignee.

Logistics research normally omits human involvement in the processes. This simplification is normally needed, but human involvement is decisive for the contextual understanding of this wicked problem. Human involvement can be divided into two different categories - perpetrator and part of the transport network. Almost all crimes (and antagonistic threats) are a deliberate or unintentional violation of law by a human. In some cases, the violation will be performed in the name of an organisation (company, association, or even authority), but even then the responsible humans are considered as perpetrator. Therefore, the human involvement on the perpetrator’s side is undisputed. Humans as a part of the logistics system is in practical terms undisputed, while normally considered only as the element that follows and executes...
the procedures within the transport chain. Papers F and G address human involvement in relation to different procedures and security. Both papers use the term security culture to describe the relationship between the needs and demands for security from a terminal worker’s point-of-view.

Paper H addresses the implementation of the ISPS code in Swedish ports and the impact it had on regular port activities. This paper illuminates the relationship between security and other processes in the transport chain. Although the initial reason for the ISPS code was terrorism, other security-related issues such as smuggling, theft, and piracy can be addressed by its implementation. The most important impact of the code is the increase of the security level in ports. Better control of the port area, restriction of unauthorized access, and a better working environment are examples of effects of the implementation of the ISPS code on ports and port activities. Paper H states that the ISPS code has advantages and disadvantages that should not overshadow its benefits, but should be considered to make its impact as effective as possible. The disadvantages are higher operation expenses and high implementation costs, but without a predefined model for cost distribution depending on the ISPS code, it is difficult to stipulate an economic result.

4.2. Paper A: The displacement effect in cargo theft

Purpose and overview

Today there is a significant problem with the theft of cargo worldwide. It is estimated that theft represents losses of at least US$10 billion per year in the United States and US$30 billion worldwide (Barth et al., 1998). The theft of cargo value for the EU is estimated to be €8.2 billion annually, an average of €6.72 per trip when allocated to all transports (EP, 2007). The effects from cargo theft incidents are often misunderstood and underestimated. Preventive measures have been implemented to mitigate the problem of cargo theft, but it persists. The purpose with the paper is to analyze and explain why cargo theft continues in the transport network despite all implemented countermeasures.

The research is based on a logical deductive hypothesis using theories from several scientific fields. Then, this hypothesis is tested empirically. Credibility is substantiated by independent official statistical sources and verified with open-ended qualitative interviews and a quantitative, comparative, and geographically controlled survey.

Main findings

The source of risk for cargo theft in the transport network comes from theft opportunities. These opportunities are highly specific and concentrated in time and place because of the required scheduling and fixed assets of normal activity in the transport network. The risk for cargo theft can be reduced by initiating resilient countermeasures that focus on reducing theft opportunities. These countermeasures are meant to change the characteristics of cargo theft, or, more correctly, change the outcome of a potential perpetrator’s decision process. If a potential perpetrator can change the target, method, place, or time, they will do so within their capability. The theory of crime displacement in the transport network states that within a potential perpetrator’s capability, they will change their criminal pattern in response to countermeasures implemented by the business. Of the six displacement types, a change in place and modus operandi are the easiest to measure and establish. There has been a lesser change in the type of products stolen from the transport network. This supports the fact that it is not the
thieves but the buyers of stolen products that govern the choice of target, while the potential perpetrators decide where and how to acquire the products. The crime displacement effect may be one likely explanation for this development.

The common sense belief in crime displacement effects within the transport network is based on macro-level statistics which clearly indicate changes in theft patterns and preventive measures taken by businesses. The prevalence of the belief that perpetrators always attack the system in the weakest point is an attractive common sense conclusion, but as indicated by the research presented in this paper and several other papers, the causal relationship between the perpetrator’s decision process and crime preventing measures is difficult to verify. This fulfils Hesseling’s statement (1994) that “crime displacement is a possible, but not inevitable consequence of crime prevention. Further, if displacement does occur, it will be limited in size and scope”. The common sense feeling about crime displacement theory in the logistics business needs to be modified, because total and partial crime displacement are different things and common sense is attracted to the idea of total crime displacement. For practical theft prevention in the transport network, the total displacement idea seems useful, but it is more useful for the locals to understand and know about modus operandi, perpetrator motivations, etc., in order to introduce the right theft prevention features. This paper has demonstrated that causality in crime displacement is difficult to establish. The same conclusion about the validity of the crime displacement theory has been presented in several other papers.

4.3. Paper B: Using business complexity to handle supply chain risk: dealing with borders of cargo liability

Purpose and overview

The international trading system depends on the effective transport of goods. During a transport from consignor to consignee, various things can occur that affect the quality of the transport. To attain an effective and smooth transport, several companies normally are involved because each company provides their core competence and activities to the flow of products. When something happens with the transport, one of the companies involved is considered responsible for the cargo. That company is the one that should investigate the incident and take proper action according to the agreements with the cargo owner. However, while logistics theories often are based on simplifications such as objectivity, rationality, and determinism, real-life logistics practice is characterized by last-minute changes and rearrangements due to people’s interpretations, accidents, changes in customer demand, machine and computer breakdowns, mistakes, and thefts. The paradox of cooperation/competition is found in logistics. It is based on striving for the “ideal” cooperative situation of a supply chain as a single unity with unifying goals, and in that drive, subjectivism, power, and conflict avoidance are hidden.

To provide explanations and understanding of how logistics business actors contribute to and use business complexity to handle supply chain risk by using cargo liability regulations to minimize negative business impact. The research is based on a system-theoretical approach that emphasizes a holistic view instead of the characteristics of the parts. The research method used in this paper is deductive. The analysis is based on complexity theory with regard to logistics business actors’ cargo liability toward the goods owner in the case of cargo theft.
Main findings

Insights from complexity theory guide the search for guiding principles to describe the behaviour of the system (Gault et al., 1996). To think in terms of complexity means to appreciate the idea that every change affects, in non-linear ways, other parts of the system. Complexity theory gives us a system understanding based on subjectivity and paradoxes instead of objectivity and rationality in interaction between actors (Macbeth, 2002). Complexity is closely related to uncertainty and the underlying principles of determinism and predictability are desirable for business. Certainty in business means that every factor is fully deterministic and the outcome will be fulfilled in a precise manner. However, uncertainty is simply a key characteristic of any economic activity (von Oetinger, 2004) and with uncertainty comes risks. A major consequence of uncertainty in business is that each actor, as rationally as it can from its subjective perspective, tries to control and reduce uncertainty.

According to Wang and Rouch (2000), risk transfer is a common strategy to control risk. The basic idea is that transferring the risk to someone else reduces personal risk substantially by using different types of contracts. In the freight industry, liability insurance is one of the best examples of the risk transfer strategy. The key element in liability insurance is the contract between the parties involved. In order to simplify business relationships, several conventions have been developed (e.g., CIM, CMR). If nothing else is contractually decided, these conventions are contractual agreements. According to Stöth (2004), the key element in all types of liability contracts is the use of clear and distinct borders of responsibility. This makes it easier to establish who is responsible if something unexpected happens. Also, the contract should account for what this responsibility means, something the CMR convention covers. The key element of liability insurance is that goods owners take a major of the risk if nothing else is decided (Stöth, 2004). According to Garrett and Marshall (2003), a common risk strategy for an actor is to own only a minor part of the equipment they use. This depends mostly on the fact that the risk for ownership is transferred.

Managing a company in a way that avoids the cons (cost and risk) and increases the pros (revenues and profit) is good business. The special case of avoiding economic impact from a cargo theft incident can be illustrated by assumptions derived from complexity theory in the transport network, i.e., subjective rationality in the local context. This will be shown in the old maid game as exemplifying strategy for the actors’ behaviour. The old maid game strategy is strategically defensive and aims only to avoid loss, not to generate income. The effectiveness of this strategy depends on the number of participants within the game. The basic idea is to hide in numbers. This may also be expressed as, “the more participants, the more effective the strategy” The game of old maid is not played exclusively within the transport network to avoid the economic impact of a cargo theft incident—it is useful in many more situations. The old maid game strategy is a way to minimize personal business risk as soon as the number of actors (including insurance policies and companies) increases. The strategy may not be spoken by each actor, but the actors will play their part in the overall business process to some extent according to the strategy. A key driver of this development is the endeavour of the actors to avoid fixed cost to minimize the risk of ownership (Marshall, 2003).

The result of this paper also may provide explanations for why supply chain collaboration is difficult to obtain. For those actors that are good at the game, it is rational to live in a greater complexity because their losses can be minimized and investments improved—at least in the short term. While most supply chain management literature communicates suggestions and results based on assumptions such as objectivity and rationality, complexity theory provides
another set of assumptions (e.g., subjective rationality, indeterminism, complexity, emergence, and self-organisation). These assumptions are more suited to a socio-technical and socio-economic context, such as supply chains, where humans and the emergent phenomena coming from their interactions are involved and central to the activities.

4.4. Paper C: Differences in stakeholder opinion regarding antagonistic gateways within the transport network

Purpose and overview

This paper addresses the vulnerability in the global flow of goods and the preventive measures taken to reduce this vulnerability. These transports have become more vulnerable. According to Svensson (2000), vulnerability is “the existence of random disturbances that lead to deviation in the supply chain of components and material from normal.” The outcome of this disturbance also should have a negative effect on the companies involved (Svensson, 2000). This definition contains two difficulties: “random disturbance” and “from normal.” The term “random disturbance” indicates that the company does not control the change, while the term “from normal” indicates there is such a thing as a normal or scheduled situation. All stakeholders have different views of and commitments in the supply and transport chain. In this study the research questions are based on these circumstances. The first research question (RQ1) hypothesizes that these differences demonstrate the various views and opinions stakeholders have about theft and smuggling as threats against their logistics businesses. The second question (RQ2) will extend this by suggesting that these differences can be linked to the attitude about introducing logistics security programmes. Using methodology triangulation (Mangan et al., 2004), this paper focuses on the different attitudes and experiences in relation to antagonistic gateways, depending on stakeholder background, and therefore strengthens the logistics knowledge base. The study is descriptive and explanatory. As a consequence, this paper intends to describe and explain the differences in stakeholder opinion regarding antagonistic gateways within the transport network.

The researcher conducted a survey that asked respondents to provide their opinions in relation to 20 statements. The study was based on answers from 30 companies and organizations. The people surveyed were all experts and practitioners in this area. The respondents could choose one of the following four answers: agreeing “strongly,” “weakly,” or “not at all” with “no opinion” as the fourth option. The respondents’ combined answers (mean values) were then presented to two groups for comments and validation of the result. Both groups verified that the survey accurately represented the problem of antagonistic gateways within the transport network. The two groups also verified that the conclusions drawn from the 20 statements were valid for the business. Some statements were more concerned with addressing attitudes; therefore, the answers from the survey must be used in moderation.

Main findings

An antagonistic gateway is an informal and hostile gateway that adds or removes goods from the network. Theft (exiting) and smuggling (entering) are illegal and antagonistic business processes that are autonomous or semiautonomous and done by perpetrators that act from a rational choice perspective (Sarnecki, 2003). When a product changes from the legal side to the illegal side or vice versa, it uses a gateway or crossover point. This gateway is chosen or created to minimize the risk of discovery with regard to normal business constraints such as cost, time, and reliability (Ekwall, 2007). In the aftermath of the World Trade Center terrorist
attack, several new security programmes were launched to protect the international cargo flow from abuse for criminal intentions (primarily terrorist) without compromising supply chain efficiency.

This paper focuses on stakeholder opinions about the existence of antagonistic gateways within the transport network, and demonstrates that there is a difference in opinion among stakeholders within the transport network. These differences can be explained by variety in stakeholder background and their position relative to the flow of goods. The recent development in the global flow of goods has been targeted by security programmes to prevent terrorist attacks that create a logistics disturbance and affect society. The development of new and additional security programmes that address security issues within the transport network will bring attention to certain processes or stakeholders in the transport chain; hopefully it will also reduce the problem of antagonistic gateways. These differences have to be taken into account when designing secure gateways or introducing logistics security programmes within the transport network.

4.5. Paper D: The role of temporary storage from a supply chain perspective

Purpose and overview

Today’s demand on high supply chain performance requires more awareness of supply chain risks and uncertainty. The purpose of this paper is to analyse the role of temporary storage in the transport network from a supply chain perspective. The primary research question is what purpose or role temporary storage plays and whether the temporary storage concept can help reduce risk and uncertainty in the supply chain. The research method is deductive; therefore, a hypothesis is developed from existing theories using logical deduction. The perspective is a system theoretical approach toward logistics. Then the theoretical findings are verified by two case studies.

Main findings

A flexible supply chain can respond to changes in internal and external factors that affect performance. A supply chain with flexibility and the ability to respond to change is called a resilient supply chain. A resilient supply chain is designed to effectively handle risks and uncertainties that may threaten supply chain performance. The causes of a disturbance and its consequences can be described in risk terms, even if they are deliberate. The important part of risk thinking in a supply chain perspective is impact reduction or minimizing the total risk for disturbance. The stronger the linear relationship between cause and effect, the better the risk management approach for reducing disturbance. Traditional risk management is better to handle risk (quantifiable threats/problems) and security is better to handle uncertainty (unquantifiable threats/problems). The present trend of leanness and low inventory levels combined with the outsourcing trend puts new demands on transport skills and functions. The lower inventory level reduces the robustness in the supply chain against disturbances. Then, in case of a disturbance, the supply chain will shut down quicker and with a higher cost attached than it would have otherwise.

The function of temporary storage is twofold. First, it is a place where physical goods wait for a short period of time to achieve the sometimes-necessary elasticity for the scheduling of the supply chain or transport network. Second, for legal and other reasons, cargo carriers need to
park, refuel, and rest. Temporary storage is located between nodes in the transport network and acts as a supply chain disturbance neutralizer, reducing risk and uncertainty within the supply chain. The use of temporary storage also means exposing the transport to a larger theft risk. To avoid supply chain disturbance and increased theft risk there are three solutions: first, better and more exact scheduling of delivery time; second, availability of secure parking spaces when a resource needs to make a temporary stop; third and the most suggested reductive measure is to utilize tracking and tracing systems. The reductive measures can work together and combined they can help reduce risk and uncertainty in the supply chain.

Transfer of risk is contingent upon the agreed transfer of ownership, the insurance situation, and whether the principles of crime displacement are applicable. Isolation (consequences do not affect the object studied) and segregation (an adverse event cannot cause domino effects) may be affected by technological means. The use of secure parking spaces when a resource needs to make a temporary stop, the use of hard-body lorries and trailers, and intelligent locking devices, etc., contribute to the protection of the goods. Supervision and rescue may be affected by using tracking and tracing systems, which is the most commonly suggested reductive measure. Various risk control options can be applied synergically and as a combined toolbox contribute to reducing risk and uncertainty in the supply chain.

4.6. Paper E: The risk for detection affects the logistics system setup for cargo smugglers

Purpose and overview

The purpose of this paper is to analyse the similarities and differences in the design of logistics systems with respect to the legality of the transported goods. The legality of goods is a vital factor when taking the goods from point-of-origin to the customer. From a simplistic point of view, the goods can be legal or illegal, but it is sometimes difficult to establish the legality in reality. This gives three stages of legality of the goods: legal, illegal, and undefined (grey zone mixed). The legality of goods differs from place-to-place and time. This means that a certain product can be legal in one geographical area and illegal in another. Therefore, the demand for an illegal product potentially will be supplied from a different logistics system, depending on the risk of discovery by authorities or other organisations. Using a systems analysis approach based on cases and supply chain theory, this paper discusses the elements that constitute the respective logistics systems designs based on legality. The triad logistics setup provides a good theoretical foundation to understand how the legal transport network is abused by criminal businesses. This paper demonstrates that a filtration of information regarding shipped products is the primary tool to successfully abuse the legal transport network.

Main findings

The primary target of illegal goods is the black market. The black market consists of places and situations where products with dubious or no legality are traded for money. This market is subject to the same forces of supply and demand as legal markets (FIA, 2001). The buyer of these illegal products is everywhere (Johns et al., 2003). The smuggling of products does not necessarily mean that the product is illegal everywhere. What is legal in one country can be illegal in another. A problem linked with smuggling is the manufacturing of products without intellectual rights, or the production of counterfeited goods. Everything that is produced can be reproduced by someone else. In terms of contraband this simply means that everything can be a counterfeited product (IACC, 2005). Then, illegal products are distributed by trade routes
and port activities in the same way as legal products (Naylor, 2004). The pollution of illegal products in the legal transport network is largely agreed upon as a serious problem. The most common countermeasure against smuggling is inspection of cargo carriers when they cross a national border. These inspections and their existence create disturbances in the transport network, even if no illegal product is discovered. The current strategy is to prevent illegal products from entering the transport network by creating secure trade lines. The idea of secure trade lines is evident in supply chain security programmes such as AEO, C-TPAT, etc. This strategy also aims to reduce custom inspection disturbances in legal business. Naturally, the legal business companies are not pleased with the competition from black market actors. They may not be pleased with legal competition either, but that is another question. The striving for better business deals and the globalization trend that started centuries ago has embedded illegal actions within legal markets (Naylor, 2004). This implies that the old black markets have been integrated with legal transactions; today the markets can be described as containing every shade of gray when referring to the legality of the markets as a whole (Naylor, 2004).

The difference between illegal and legal logistics flow in its simplest form can be defined as a unique constraint affecting only the illegal flow that does not exist in the legal system. The unique constraint is the risk of being discovered by authorities and therefore suffering a flow stoppage; it should lead to a different setup of the logistics system for the illegal supply chain to fulfill its scope of logistics. Minimising the potential effects from constraints in the transport network allows illegal supply chains to obtain better illegal business deals. According to Naylor (2004), the aspiration for better business deals together with the general globalization trend has embedded illegal actions within the legal markets. Therefore, this development should be visible in the global flow of goods, but illegal logistics system setups should differ from the normal (legal) setup, depending on the risk of detection.

Logistics activities use the same infrastructure, whether the goods can be categorized as legal or illegal. The economy of scale in logistics has made it more efficient and faster to conceal illegal goods in legal shipments. The need for speed and low cost control sets the trend in the way of doing business on both sides of the law. Regarding illegal logistics resources for transport, there are still trucks with only illegal goods in the shipment while large cargo carriers (ocean-faring ships) are not likely to use illegal infrastructures but instead will use trucks. The highest level of logistics, the flow of material, and the difference between black and white logistics is most evident here because it is easiest to distinguish legal from illegal goods.

The ability to establish the legality of a certain product is necessary to correct balance constraints and minimize the potential risk for disturbance in the transport network. In terms of discovering illegal goods in legal logistics flows, the need for correct information is crucial. The nature of the illegal goods governs the choice of logistics setup, e.g., using concealed shipments or a company’s logistics system setup. The more difficult it is to distinguish illegal products from legal, the more likely they are to be transported in the legal logistics system. By providing reliable false information to the legal logistics company, it is possible to increase the likelihood of an illegal shipment reaching its consignee.

Purpose and overview

In this article we investigate the meaning that terminal workers within the transport sector ascribe to their responsibility and organisational conditions to handle risks of theft. The concept of frames and Mary Douglas’s grid/group model are used to analyse the security culture among workers at three Swedish freight terminals and how culture directs their understanding of responsibility for a potential and daily security problem. According to above information, it could be assumed that terminal workers will frame theft as a problem handled either by self-governed workers in the organisation or by the top management in charge of industrial procedures of work, limiting individual responsibility. However, by using Douglas’s grid/group model, we also may elaborate further variations in their frames of responsibility.

The study is based on qualitative interviews motivated by the investigation of the meaning that terminal workers ascribe to issues of theft. The purpose is not to measure the causal strength in certain perceptions of risk and organisational structures for example, but to understand and define the way terminal workers frame potential thefts at work (Kvale, 1997). Focus is placed upon the pronounced content as well as the presence and absence of certain qualities in their framing (Kelle, 1995). Furthermore, our intention is not to present an empirical picture of how security is received generally within the transport sector. In total, 15 interviews were done at three freight terminals (five interviews at each terminal). Each interview took 30–45 minutes. The interviews were conducted during work time, which made it difficult to lengthen the conversation. The workers or respondents were all permanently employed, had low education level and functioned at the shop floor level; only two were women. Empirical variation was increased by tasks, length of employment, and age (Seidman, 1998). Furthermore, the terminals belonged to two international companies, of which one company had a decentralised security organisation and the other a centralised security organisation, i.e., two terminals had central security staff to consider.

Main findings

In this study, all workers expressed a common industrial frame of security at work. In accordance with the grid/group model they described a legitimate hierarchy and a wish to keep the organisation and working groups honest and stable (Douglas & Wildawsky, 1983; Engdahl, 2003). Rather than referring to autonomous individuals conducting complex jobs in an ever-changing transport network, they framed themselves as decent blue-collar workers at the bottom of the organisation. They complained about repetitive tasks, bad working conditions, and poor communication with the top management, which limited their own initiative. However, it was important that management followed established routines and procedures (Mars, 1997). Despite the differences mentioned in the industrial frames, no respondent wanted a security organisation in which flexible individuals replaced hierarchical top-down control.

The respondents described it as a complicated, even discouraging, necessity. However, contrary to the respondents from the medium-sized terminals, they also wanted more knowledge and wanted to be capable of handling the problem of theft themselves. Once again, we can conclude that an industrial and hierarchical security culture does not exclude frames of daily security at work in which initiatives from the shop floor and aspects of the self-governed worker are expected. An important question for further research becomes how much space
such a shop floor responsibility may be given under hierarchical circumstances and in what sense the security culture then depends on external relations.

4.8. PAPER G: Security culture and transport network terminal activities

Purpose and overview

The increasing trend of globalisation has led to an increase in logistics activity. The international trading system depends on the effective transport of these goods, and these transports have become more vulnerable. In many cases, this vulnerability can be described as unwanted effects in the supply chain caused by internal or external forces that create disturbances larger than the supply chain is designed to handle. In the report CEN (2006), security measures are categorised into three approaches: psychological, systematic, and technology. The psychological approach establishes awareness among personnel working in the transport network. High awareness or alertness depends on interaction and involvement of personnel in policy and business processes. Therefore, good awareness about the problem of cargo theft must be a part of the unwritten regulation of behaviour, or in other words, part of the company’s culture with regard to cargo theft problems. Several of the other supply chain security programmes such as C-TPAT, CSI, AEO, etc., emphasize the need for employee awareness to increase the overall security level. The awareness and the way things are done can be called the security culture. The purpose of this paper is to analyse the security culture among terminal workers in a transport network, with the background of the increasing use of security awareness advocated by several international supply chain security programmes in recent years. The data is collected through qualitative interviews at three different terminals.

Main findings

Neither of the two companies was willing to share with researchers their statistics regarding thefts in the three terminals for business reasons. The security organisation is similar in both companies and both consider it secondary to the operational structure and instructions. In every terminal there is an appointed site security officer (SSO) with operational responsibility for security in the terminal area. Common to both cases is that the cost for security is in each terminal manager’s budget and the CSO is placed in a centralized staff function to the managing director.

Risks can emerge from within the organisation and the environment. Logistics literature agrees that uncertainty should be reduced as much as possible. The chase for equilibrium and stability in logistics may negatively affect the establishment of awareness of criminality problems within the logistics business unless the interaction and involvement of personnel in policy and business processes are encouraged by management. This need increases as potential perpetrators become more sophisticated, which also reduces the possibility of effectively using statistical theft prevention methods. This call for a more holistic approach toward the design of logistics business processes, in accordance with the expression, “go with the flow.”

With the background in the risk ranking for three terminals and 15 qualitative interviews, it is easy to conclude that riskier surroundings affect the security culture among terminal workers, but how this influence affects the security efforts depends on several factors. The security culture also depends on the organisational complexity in each terminal/company. In order to coordinate security in global and complex organisations, self-conducted staffs are increas-
ingly important. This research indicates that if the surroundings are more uncertain, then one cultural response is to have a small drafter toward the fatal frame of the grid/group model. The right response and attitude from management may hinder a fatal disbelief in the organisations ability to prevent criminality.

4.9. **PAPER H: Impacts of the ISPS code on port activities – A case study on Swedish ports**

**Purpose and overview**

Following the terrorist attacks on the World Trade Center in the United States and the Limburg oil tanker in Yemen, the International Maritime Organization (IMO) agreed to develop new measures related to the security of ships and port facilities. In December 2002, the IMO defined a new rule for security issues for ships and port facilities, the International Ship and Port Facility Security (ISPS) code. The ISPS code was entered into force on July 1, 2004, to reinforce maritime security and prevent similar terrorist acts against shipping.

The code contains two parts: the first part (A) is compulsory while the second part (B) is a guideline when implementing the security provisions in part A. Basically, the ISPS code has been applied to safeguard maritime transport security by ensuring the security of ships and port facilities, onboard the ships, and at the port/ship interfaces will always be in place. The implementation of the ISPS code involves changes in the physical design of port area security and changes in general port activities. There are always concerns that a security rule goes far beyond what is needed and then becomes an obstacle instead of being a good incentive (D’Addario, 2006). This paper addresses the effects of the implementation of the ISPS code on ports in order to clarify any obstacles or good collateral benefits on port activity.

**Main findings**

The ISPS code’s main mission is to address security issues in maritime transport. Although the initial reason for the ISPS code was terrorism, other security related issues such as smuggling, theft, and piracy can be addressed by its implementation. Increasing the security level in ports is the most important impact of the code. Better control of the port area, restriction of unauthorized access, and a better working environment are examples of the effects that implementation of the ISPS code has on ports and port activities.

In addition the advantages of the ISPS, there are some disadvantages which should not overshadow its benefits, but should be considered to make its impact as effective as possible. The disadvantages are higher operating expenses and a high implementation cost. This research supports the findings of the other authors (Stevenson, 2005; McNaught, 2005) that one of the main problems with the code’s implementation is the lack of a predefined model for distributing costs depending on the ISPS code.

The general hostile and illegal threats against ports in Sweden are considered low, and many ports may have a lower need for security than the ISPS code recommends. Therefore, the implementation of the ISPS code is probably considered a compliance issue and mostly a cost increasing feature instead of a security increasing programme, regardless of any collateral benefits. This paper shows the smaller ports in Sweden had a lower level of ISPS compliance before its implementation. Therefore, their investment and overall effort to achieve ISPS compliance was larger than the bigger ports.
The conclusion from this research can be presented in terms of advantages and disadvantages of the implementation of the ISPS code as follows:

General advantages of the ISPS code:

- Better safety and security and lower risk
- Better control on port’s area, goods flow, and personnel
- Better documentation (having unit standards for documents)
- Better working environment

General disadvantages of the ISPS code:

- Work slows progress
- More paperwork
- More costs
- More administration work

The ISPS code affects a large part of port activity; the research clearly indicates that 17 percent of the ports participating believed the ISPS code did not have any disadvantages, while only 7 percent said it had no advantages. A majority of the participating ports (80 percent) noted an increase in security level, which is the main goal of the ISPS code. Consequently, factors such as security level could be more powerful in satisfying the port administration in parts of the world other than Sweden. Therefore, we can conclude that the satisfaction with the ISPS code is related more to local port external factors than to the ISPS code itself.

Overall, the ISPS code is like a train that is moving while railroad tracks are being laid. There were many issues such as human rights matters and models for cost distribution that needed more consideration before its execution.
4.10. Result of appended papers

The combined results of these appended papers are used to answer the research questions and substantiate the contextual understanding required to handle this wicked problem. In Table 19 the results from the different papers are presented in relationship to the research questions in this thesis. The results are presented with a statement or comment to provide a general view of the wicked problem of antagonistic threats against the transport network.

<table>
<thead>
<tr>
<th></th>
<th>RQ1</th>
<th>RQ2</th>
<th>RQ3</th>
<th>RQ4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper A</td>
<td>- Crime causality is hard to establish</td>
<td>- Theft opportunity</td>
<td>- Situational crime prevention</td>
<td>- Crime displacement</td>
</tr>
<tr>
<td>Paper B</td>
<td>- Borders of liability</td>
<td>- Old maid game strategy</td>
<td>- Negative for collaboration</td>
<td>- Increased business complexity</td>
</tr>
<tr>
<td>Paper C</td>
<td>- Mode dependent</td>
<td>- Different stakeholder perspectives</td>
<td>- Anti-terror programmes</td>
<td></td>
</tr>
<tr>
<td>Paper D</td>
<td>- Risks and uncertainty in both supply</td>
<td>- JIT approach</td>
<td>- Slot time usage</td>
<td>- Secure parking</td>
</tr>
<tr>
<td>Paper E</td>
<td>- Gray market</td>
<td>- Risk minimizing</td>
<td>- Smuggling</td>
<td>- Information filtration</td>
</tr>
<tr>
<td>Paper F</td>
<td>- Employee awareness</td>
<td>- Environmentally dependent risk</td>
<td>- Leadership</td>
<td>- Self governed employees</td>
</tr>
<tr>
<td>Paper G</td>
<td>- Employee awareness</td>
<td>- Procedures</td>
<td>- Holistic approach</td>
<td></td>
</tr>
<tr>
<td>Paper H</td>
<td>- Physical security</td>
<td>- Increased cost</td>
<td>- Holistic approach</td>
<td>- Innovative use of technology and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>procedures</td>
</tr>
<tr>
<td>Combined results</td>
<td>- Theft opportunity</td>
<td>- Risk transfer</td>
<td>- Negative for collaboration</td>
<td>- Holistic approach</td>
</tr>
<tr>
<td></td>
<td>- Mode dependent</td>
<td>- Risk prevention</td>
<td>- Anti-terror programmes</td>
<td>- Leadership</td>
</tr>
<tr>
<td></td>
<td>- Gray market</td>
<td>- Employee awareness</td>
<td>- Environmental dependent risk</td>
<td>- Information filtration</td>
</tr>
<tr>
<td></td>
<td>- Risks and uncertainty in both supply</td>
<td>- Borders of liability</td>
<td>- Environmental dependent risk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and transport chain</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 19: The result of the appended papers and the research questions

The 16 different statements that constitute the combined results from papers appended to this thesis all contribute to improving the contextual understanding that is vital for this thesis. These statements are explained more in detail in Chapter 5.1.
5. Analysis

This chapter contains an analysis of the appended papers within the frame of reference.

5.1. Research questions - analysis

The analysis of each research question is based on the results from the appended papers presented in Chapter 4.10 (see Table 19).

RQ 1 What are the characteristics of antagonistic threats against the transport network?

-Threat opportunity: The characteristics of antagonistic threats can be simplified because there are opportunities and motivated perpetrators. The perpetrator’s motivation is by itself a very complex issue and is only mentioned in Chapter 2.10.3. The opportunities can be defined as the unique combination of object, place, time, perpetrator position, and lack of security (Chapter 2.10.1). Different perpetrators evaluate opportunities differently; some perpetrators create the opportunity they need (professional perpetrators) while others use the moment (opportunistic perpetrators). Common to all perpetrators is that opportunity is a dynamic and vital element to understanding the characteristics of antagonistic threats against the transport network.

- Transport mode-dependent characteristics: Different modes of transport provide various threat opportunities and security gaps. A comparison between the modes of transport with regard to transported value, weight, and losses is presented in Table 20. The statistics Table 20 with regard to weight and value are valid for Sweden while the losses are valid globally. This divergence leads to a lower credibility but the result is unequivocal and the analysis is valid.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Road</td>
<td>72</td>
<td>81</td>
<td>74.6</td>
</tr>
<tr>
<td>Rail</td>
<td>14</td>
<td>7.6</td>
<td>0.8</td>
</tr>
<tr>
<td>Sea</td>
<td>13.2</td>
<td>2.7</td>
<td>1.5</td>
</tr>
<tr>
<td>Air</td>
<td>0.4</td>
<td>7.1</td>
<td>23.1</td>
</tr>
<tr>
<td>Other</td>
<td>0.4</td>
<td>1.6</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 20: Transport mode theft characteristics

The risk for loss varies greatly between the modes of transport. There is no surprise that truck and air combined represent 97 percent of all loss (but only 88 percent of the value), while rail stands for 7.6 percent of the value but only 0.8 percent of the losses. The high value and hot products (Chapter 2.10.8) use road and air transport instead of rail. This difference helps explain the variances in theft opportunities depending on mode. The three elements of crime (perpetrator, object, and lack of guardian), along with assets and infrastructure dependencies in the transport network (Chapter 2.9.3), provide a broad spectrum of opportunities that are closely linked to the modes of transport (Chapter 2.11.3). Therefore, threat opportunities are transport-mode dependent.
- **Gray market characteristics**: The market where products with dubious or no legality are traded for money is called the gray market in many cases because customers do not know if the product is legal or illegal. The primary goal for economically driven antagonistic threats is for the perpetrator to make a profit from the crimes (cf. Mankiw, 1997). Whether the crime is classified as theft, smuggling, or counterfeit branded products, the key element is the transformation process from object to money. This is achieved in the gray market, which is subject to the same forces of supply and demand as legal markets but has an additional risk factor for the parties involved (Chapter 2.1.3). This establishes a different (to varying extents) supply chain design (Level 1 in Chapter 2.8.3) and a different transport network configuration (Level 2 in Chapter 2.8.3). Therefore, organisations and inter-organisational networks (Level 3 in Chapter 2.8.3) depend on the wider environment in which the gray market and its supply chains exist (Level 4 in Chapter 2.8.3).

- **Risks and uncertainty in the supply and transport chains**: The difference between risk and uncertainty is that risk has a quantifiable measure for future events and uncertainty does not. Therefore, risks can be regarded as quantifiable uncertainties (cf. Water, 2007). Some threats are very difficult to quantify, but they are still possible. With a wicked problem it is important to concentrate on possibility rather than probability, because a classic quantifiable problem with a direct relationship and the continuous variables of cause and consequence needs to be described with possibilities and vulnerabilities as alternative relationships to accommodate multiple perspectives.

The supply chain is a better term than transport chain because transport only physically integrates the supply chain with the fulfilment of the supply chain’s transport demands. Therefore, the supply chain risk consequences can be amplified or absorbed by supply chain control mechanisms such as batch sizes, inventory safety margins, decision rules, and policies regarding order quantities. With this said, risks/uncertainties in the transport chain can be amplified or absorbed by overall supply chain risk with mechanisms such as route planning, track and tracing, secure parking, and rigid scheduling. There is a very complex relationship between risks/uncertainties in supply and transport chains and within this countless threat opportunities can be found, created, exploited, and prevented.

**Conclusion**

The wicked problem of antagonistic threats against the transport network changes appearance depending on which stakeholder delivers the judgments and interpretation of the problem. Therefore, the necessary common ground for describing the problem is missing or described differently and a separation of material and non-material structures of the logistics business is impossible. The antagonistic threat triangle (Chapter 2.12.1) illustrates the elements, events, and relationships within the supply chain risk context that explains and simplifies the understanding of antagonistic threats.

Economically driven antagonistic threats are subject to the supply and demand forces of the gray market, while non-economically driven antagonistic threats are linked more too political, ideological, and/or religious issues. These driving forces and opportunities such as the unique combination of object, place, time, method, perpetrator position, and security (or lack of) contribute to the risk and uncertainty in supply and transport chains. The characteristics of antagonistic threats against the transport network can be described with a few guiding principles that describe the behaviour of the system. Therefore, the understanding of the characteristics of antagonistic threats is based on subjectivity and paradoxes instead of objectivity and ra-
tionality in interaction between actors/elements/stakeholders. The handling of antagonistic threat against logistics is a balance between the desired supply chain performance and reducing opportunities while avoiding potential crime displacement.

RQ 2 How are these antagonistic threats organised and managed today?

- Risk transfer: Risk transfer is a common strategy to achieve risk control. The basic idea is that transferring the risk to someone else reduces personal risk substantially through different types of contracts. The use of insurance policies is a natural and considerable part of supply and transport chain activities in particular. The key element is liability which governs in several international conventions and regulations. The other main strategy is risk prevention, normally achieved with the extended use of physical security and employee awareness.

- Risk prevention: The basic risk reduction method is prevention. Risk prevention has three different components - the right management approach, technology, and re-engineering operational processes. The right management approach refers to the general awareness and understanding of the wicked problem of antagonistic threats by everyone from senior management to seasonal employees and the right organisational set up. Risk prevention strategy is closely linked with technology features. These solutions also can be referred to as physical security countermeasures. These countermeasures include fences, locks, seals, guards, CCTV, and other security systems. The objectives for these types of countermeasures are to make the theft harder and riskier to commit. Re-engineering operational processes within the organisation’s responsibility and in other parts of the supply chain and transport network is important to security. A simple re-engineering of a few features or processes can reduce opportunity and perpetrator motivation.

- Employee awareness: The next important countermeasure is the control and trust of employees in the company. This method targets internal theft and can be subdivided in two parts: present employees’ supervision and new employee reference checks. These methods are not sufficient without employee education to increase the awareness of the different types of antagonistic threats and to clarify operational and organizational structures/procedures to handle these threats.

- Borders of liability: Typically, the key element in liability insurance is the contract between the parties involved. In order to simplify business relationships, several conventions have been developed (e.g., CIM, CMR, and Incoterms 2000). If nothing else is contractually decided, these conventions are contractual agreements. The core of all liability contracts is the use of clear and distinct borders of responsibility. This makes it easier to establish who is responsible if something unexpected happens. Also, the contract accounts for what this responsibility means. The incentive for participating in a business deal or process for each individual stakeholder can be found in ratified borders of liability.

Conclusion

Today, the management of antagonistic threats primarily uses two main strategies/methods - risk reduction and transfer. The key element in risk transfer strategy is borders of liability according to the rule-of-thumb statement, “no liability-no problem”. This is an inadequate view of the problem because supply chain disruptions can cause problems for companies and processes indirectly. Therefore, prevention strategies also need to use the rule-of-thumb
statement, “no liability-extended problem” to understand the vulnerability for antagonistic threats and manage the potential business impact. Risk reduction strategy is based on the right management approach, correct use of technology, and the re-engineering of operational processes. They are equally important and it is their interaction that alters the opportunities for antagonistic threats in the eyes of the perpetrator.

RQ 3  What are the effects on the transport network with both regard to the characteristics and the management of these antagonistic threats?

- Negative for collaboration: The logistics literature on supply chain collaboration/cooperation advocates that the stakeholders act according to the agreement or collaborate so each stakeholder wins and the optimum combined profit is fulfilled. It is based on striving for the ideal cooperative situation of a supply chain as a single unity with unifying goals, and in that striving, subjectivism, power, and avoidance of conflict are hidden. The presence of antagonistic threats affects the will to collaborate/cooperate negatively because participation means sharing cost. If the contractual agreement between the parties involved is designed to share benefits and drawbacks in a win-win situation, then it should be possible to collaborate even in the presence of antagonistic threats.

- Anti-terrorist programmes: In the aftermath of the World Trade Center terrorist attack, several new security programmes were launched to protect the international cargo flow from being abused for criminal (primarily terrorist) intentions without compromising supply chain efficiency. The security programmes address different aspects of supply chain security and target different parts of a transport chain. The big difference between logistics security programmes is that those launched before September 11, 2001, were focused on anti-theft and issued by the business itself, while the latter were created by authorities and primarily focus on terrorism prevention. The creation of and demand for these security programmes have increased the security level of the parts of the supply/transport chain.

Environmentally dependent risk: The risk of antagonistic threats depends on assets and infrastructure (Chapter 2.9.3) or in other words the threat risk depends on the utility and movement of fixed and mobile assets. The risk for fixed assets such as terminals, warehouses, ports, and resting places depend on the local area risks. The same is true for cargo carriers such as trucks, trains, ships, and aeroplanes with the difference that the local area risk changes as the cargo carrier moves. This fact is explained by opportunity to crime statements (Chapter 2.10.1) with an emphasis on the first four opportunity principles:

- Opportunity plays a role in causing all crimes,
- Crime opportunities are highly specific,
- Crime opportunities are concentrated in time and place,
- Crime opportunities depend on everyday movements,

The last principle refers not only to the movement of the cargo carriers but to the daily behaviour of goods, personnel, cargo carriers, and infrastructure work load (Chapter 2.11.3). According to Hesseling (1994), potential perpetrators normally are limited in their mobility, adaptability, and flexibility relative to a particular crime, place, time, and method, and therefore the risk of antagonistic threats against the transport network is closely related to the local environment. This relationship between locally generated risk and transport network fluctuates depending on the primary force for the perpetrator (economic or non-economic) and the wider environment (Chapter 2.9.3) such as the economy, society, and the forces of nature.
The mapping of hot spots in the global flow of goods is a strong indication for environmentally dependent risk of antagonistic threats.

- **Increased cost**: The equipment and training necessary to fulfil security demands within different programmes and from customers’ costs money. Businesses are trying to find a model for distributing the costs of security in such a way that every participant can collaborate to solve the problem, but until that model is generally accepted by the stakeholders of the supply/transport chain, the increased cost for security will affect business margins and reduce their will to collaborate in security issues.

**Conclusion**

After the terrorist attack on the World Trade Center, authorities have launched several logistics security programmes that target different aspects of the physical supply/transport chain infrastructure and the relationship between authorities and logistics operations such as cross-border activities. The cost to implement these programmes alters the current collaboration models with regard to risk and profit sharing within the supply chain. The risk for antagonist threats depends on the local environment. This is compared with the fact that the security programmes advocate one to three security levels to solve the problem. Therefore, the security level is adjusted for security programmes instead of the local threat and security cost is higher than needed, but a standardisation of security within the supply/transport chain may result in better collaboration.

**RQ 4**  
*How can antagonistic threats be managed more effectively?*

- **Holistic approach**: The holistic approach is useful when the risk arises from the environment and a greater understanding of the cause is needed to reduce the total risk. A holistic approach also sees beyond the organisational boundaries and minimises the risk for security gaps. The holistic approach also emphasises the need for contextual understanding or investigation of the problem’s environment and minimises the total supply chain cost of antagonistic threats. The results from papers B and C indicate that the holistic approach is a theoretical product and that the practical solution is that each stakeholder primarily addresses the problem from the cost perspective and secondarily out of a holistic approach. The simplification of a holistic approach addresses the different stakeholders’ views. This approach fits the wicked problem definition well.

- **Leadership**: The human side of security is vital. This thesis only briefly addresses human involvement in logistics security (papers F and G), but it is not possible to advocate a holistic approach for security if the human side is not involved. This side normally is addressed in logistics as procedures and routines, but to have them performed as intended requires leadership from management in all levels of the organisations involved.

- **Information filtration**: The single most important element to avoiding and preventing the mixture of illegal products/goods with legal goods is correct information. This information needs to cover everything from the product itself to the stakeholders involved and the freight route. This produces vast amounts of information; therefore, a smart filtration of information is required to find illegal shipments/products/actors.

- **Innovative use of technology and procedures**: Transport security is the management approach to reducing the occurrence and impact of antagonistic threats. Transport security is
defined as the interaction between physical obstructing artifacts and the intervention of humans. The physical obstructing artifacts can be new and innovative products or older and well known products that are used with consideration of security and logistics efficiency.

Conclusion

A holistic approach is necessary to reduce the total risk for a supply chain, its processes, and stakeholders. The holistic approach also emphasises the need for contextual understanding or investigation of the problem’s environment. The management of antagonistic threats with a holistic approach requires leadership from all levels of the organisations involved for developing and implementing procedures and routines and amplifying the human side of security. The leadership aspect involves coordination and collaboration with regard to security and insurance coverage. Excellent security also requires physical obstructing artifacts that can contribute to logistics efficiency and prevent antagonistic threats. The smart use of information can separate legal shipments from illegal ones. This information needs to cover everything from the product itself to the stakeholders and freight route. This produces vast amounts of information; therefore, a smart filtration of information is required to find illegal shipments, products, or actors.

The holistic approach minimises the total supply chain cost for antagonistic threats. The results of papers B and C indicate that the holistic approach is mainly a theoretical product and that the practical solution is that each stakeholder primarily addresses the problem from the cost perspective and secondarily from a holistic approach. One explanation behind this development may be found in the ten principles of microeconomics (Chapter 2.2.1) where the sixth principle is, “Markets are usually a good way to organize economic activity” (Mankiw, 1997).

Appendix D shows the estimated cost for cargo theft in Sweden. This estimation is based on the holistic approach and therefore it is possible to claim that the combined cost for the stakeholders in Swedish transport with regard to cargo theft is higher than the total estimate. Overall, in order to manage antagonistic threats and become more effective, the stakeholders need to adopt a more holistic approach. The use of a holistic approach against antagonistic threats clearly needs more research. This idea will be addressed in Chapter 7.2.
5.2. The antagonistic threat triangle

This thesis uses several different theoretical models to describe different aspects of logistics and antagonistic threats. All models provide a different viewpoint and contribute to the contextual understanding. Simplification is a powerful tool to present basic and advanced features/elements in a complex system. Insights from complexity theory guide the search for guiding principles that describe the behaviour of the system (Gault et al., 1996). To think in terms of complexity means to appreciate the idea that every change affects, in non-linear ways, other parts of the system. The complexity theory gives us a system understanding based on subjectivity and paradoxes instead of objectivity and rationality in interaction between actors (Macbeth, 2002). The complex relationship between transports and antagonistic threats starts with the motivated perpetrator and continues with logistics functions that relate to the motivated perpetrator and elements of crime.

Interpretation of the antagonistic threat triangle can be achieved through several perspectives, which simplistically is presented as relationships between the corners and the opposite sides as well as between the corners and two adjacent sides.

Figure 21: The antagonistic threat triangle

The following perspective has been drawn from the antagonistic threat triangle:

Potential perpetrator – supply chain performance:

The relationship between a potential perpetrator and supply chain performance is the main perspective of this thesis with the limitation that the supply chain is only represented with transport needs throughout the global transport network. This relationship is complex and the problem with antagonistic threats against the supply chain performance can be defined as a wicked problem. Based on the definition of antagonistic threat in this thesis, the core element for antagonistic threats is a motivated perpetrator with hostile intentions toward the object.
and/or third party (supply chain performance) that violate international, national, or local law. The potential perpetrator is important because law violation is considered a human attribute and an antagonistic threat must be planned, executed, and understood within the relationship between a potential perpetrator and supply chain performance.

Object – crime displacement:

According the three elements of crime, the object is the sought-after reason for the potential perpetrator. The object can fluctuate depending on a large number of variables, but out of these a few can be considered dominant within the context of logistics - the goods transported, the cargo carrier, private belongings of the cargo carrier personnel, and a political value that the previous variables represent. Chapter 1.1 presents and describes these dominant object variables. If changes in the demand for a certain product/product group and the possible methods available for a potential perpetrator occur, then crime displacement is a possible outcome. The theoretical relationship between object and crime displacement is presented in Chapter 2.11 and the practical is addressed in Chapter 1.1 and Paper A.

Security – opportunity:

The relationship between security and opportunity is the predominant understanding of security in different contexts. This depends on the premise that security only can deter or repel a motivated perpetrator from committing a crime by limiting the opportunities for a certain crime. The most important thing to remember with crime opportunities is that an opportunity alone does not explain why a crime occurs because a crime needs a motivated perpetrator and opportunity to occur (Clarke et al., 2003). According to Felson et al. (1998), opportunity plays a role in causing crime, and these opportunities are highly specific, concentrated in time and place, and depend on everyday movements. These opportunities can be reduced and focused opportunity reduction can produce wider declines in crime. The real problem occurs when an organisation’s security capability is lower than the capability of the potential perpetrator. The difference between these two capabilities is the window of vulnerability (Almay, 2006) or opportunity. Proper security aims to reduce or shut that window. The theory of situational crime prevention is useful to reduce opportunity and is further addressed in Chapter 2.11.6. The theory of crime opportunity also refers to the fourth principle of microeconomics (Mankiw, 1997) - people respond to incentives - and there the degree of opportunity or incentive needed depends on the individual. The incentives could be vindication from morality, ethics, altruism, or determinism. Therefore, the relationship between security and opportunity must be understood from the viewpoint that the parties involved (stakeholders, actors, and humans) have different individual incentives to exploit opportunity that security needs to address. Consequently, security cannot be seen as only opportunity limiting but also as incentive limiting, making security a preventive factor on both sides of the opportunity (pre- and post-event) (cf. Borodzicz, 2005). This relationship is addressed in Paper E and in chapters 2.8, 2.9, and 2.11.

Security - crime displacement - potential perpetrator:

The interaction between security, crime displacement, and potential perpetrator is a complex and dynamic relationship. Security is used to change the characteristics of the outcome of a potential perpetrator’s decision process (Chapter 2.11). The theory of crime displacement in the transport network states that within the potential perpetrator’s capability, they will change their criminal pattern in response to countermeasures implemented by the business. The
common sense belief in crime displacement effects within the transport network is based on macro-level statistics. The prevalence of the belief that perpetrators always attack the system in its weakest point is an attractive common sense conclusion, but the causal relation between the perpetrator’s decision process and crime prevention measures are difficult to verify. This fulfills Hesseling’s conclusion (1994) about crime displacement, which says “crime displacement is a possible, but not inevitable consequence of crime prevention. Further, if displacement does occur, it will be limited in size and scope”. According to Saunders (2008), it is possible that “some perpetrators respond to sophisticated transport security measures by increasing their use of unsophisticated and brutal violence against drivers and terminal personnel”. A similar development is expressed by EP (2007): “The criminal organisations seem to react to the increased security with more aggressive methods”. For security in the transport network, the total displacement idea seems useful, but in reality, it is more useful for the locals to understand and know about modus operandi, a perpetrator’s motivations, etc., to introduce security features. The interaction between security, crime displacement, and potential perpetrator is primarily addressed in Paper A.

**Potential perpetrator - object – opportunity:**

The interaction between potential perpetrator, object, and opportunity appears at first to be direct and linear. The fourth of the ten crime opportunity principles states that, “crime opportunities depend on everyday movements” (Chapter 2.11.3). Stated in another way, crime opportunities depend on routines or predictability within certain boundaries, or in this thesis, the transport network as a part of supply chains. This rephrasing also includes more principles than the stated principle, implying that system predictability or routine provides opportunity for crime. In criminology, this is called the routine activity perspective (Cohen et al, 1979). The theory is a strong foundation to understand crime and opportunity for crime. The routine activities perspective argues that normal movement and other routine activities play a significant role in potential crime. This practical consequence of the routine activities perspective is that the potential perpetrator, in their pursuit of the right (desirable) object adjusts to the movement (routine) of the victim.

The opportunity depends on the perpetrator’s ability to use the routines of the object and potential guardian. In the short time perspective, the infrastructure is fixed or completely predictable. The movement of resources between terminals, factories, and other nodes also is predictable to a large extent. The routine activity perspective states that predictability in infrastructure and resource movement will significantly contribute to establishing crime opportunities. The load or the flow of material varies to a higher extent but depends on the actors in the supply chain instead of actors in the transport network. This idea will be addressed in Chapter 7.2. Therefore, the routine activity perspective provides a theoretical foundation for antagonistic activities against the transport network. Therefore, when the transport network (object) changes, so does the opportunity that may be exploited by a potential perpetrator.

**Object - supply chain performance – security:**

These three components work well together and it is using this triangle that the current development with different supply chain security programmes should be understood. The declaration is as follows: the security (supply chain security programmes and legislation) intends to guard the object from terrorist or other types of antagonistic threats, and the collateral benefit is better supply chain performance. First, supply chain security should incorporate not only theft prevention but also anti-terrorism measures. Second, the focus is now on addressing
global issues and not just local or national issues (Sweet, 2006). Third, when conducting contingency planning, the concept of crisis management should be included to obtain better resilience. Finally, security is no longer an internal corporate question but rather an issue for all actors within the entire supply chain (Closs et al., 2004). This relationship is addressed in papers C, D, F, G, and H as well in chapters 2.8 and 2.9.

Crime displacement - potential perpetrator – opportunity:

The relationship between a potential perpetrator and opportunity firmly established in criminological literature as crime opportunity is a cornerstone of all criminal behaviour (Felson et al., 1998). The most important aspect of crime opportunities is that an opportunity alone does not explain why a crime occurs. A crime needs a motivated perpetrator and opportunity to occur (Clarke et al, 2003). Simplistically stated, the three elements of crime can be reformulated as motivated perpetrator and opportunity, where opportunity is the unique combination of object and lack of a capable guardian. Reducing opportunity does not usually displace crime, but crime displacement is a possible outcome of changes in opportunity. Changes in the wider environment referred to as social and technological changes produce new crime opportunities which the potential perpetrator may or exploit depending on the outcome of the perpetrator’s decision process.

The optimize principle from microeconomics provides a guiding principle which needs to be viewed from Smith’s belief (1776) that the two sides (negative/positive effect or exploit the crime opportunity or not) neutralize each other’s influence, but if exposed to the forces of a free market, the society as a whole may benefit from individual selfishness and greed. The changes in the wider environment may provide wanted and unwanted (regardless if they are defined as a crime) opportunities. The triangulation between human driving forces (motivation), changes in opportunities provided by changes in society, and the optimize principle from microeconomics can be used to explain general business behaviour as well as changes in the wicked problem of antagonistic threats toward the global transport network.

Opportunity – object - supply chain performance:

The supply chain performance depends on the efficient movement of objects (products, cargo carriers, etc.) and can be threatened in various opportunities. This triangulation can be referred to as vulnerability. The vulnerability can, in many cases, be described as “unwanted effects” or the consequence of the risks to the supply chain. Supply chain vulnerability reflects sensitivity of the supply chain to disruption (Waters, 2007). Juttner (2005) defines supply chain vulnerability as, “an exposure to serious disturbance arising from supply chain risks and affecting the supply chain’s ability to effectively serve the end customer market.

The increasing supply chain vulnerability is an unintentional side effect of a limited view of different types of risks that may cause disruption (Waters, 2007). To reduce this vulnerability, actors and stakeholders must identify their own internal risk as well as the risk of collaboration and linkage with other actors/stakeholders (Juttner, 2005). A typical response to uncertainty and vulnerability is to create flexibility in the supply chain (Prater et al., 2001). A supply chain with flexibility and the ability to respond to changes is called a resilient supply chain. Resilience is defined by Christopher et al. (2004 - b) as “the ability of a system to return to its original state or move to a new, more desirable state after being disturbed”. Supply chain resilience includes flexibility and last minute changes to transport and production. The vulnerability of the supply chain is transmitted to the transport network because transport and
freight activities physically bring the different facilities in a supply chain together. Therefore, uncertainties and vulnerabilities in the supply chain and transport network mutually affect, contribute, and neutralize each other. In terms of the antagonistic threat triangle, this is illustrated because supply chain performance depends on objects (goods/cargo and resources) which can be exploited through a lack of security.

Supply chain performance – security - crime displacement:

Supply chain security or transport security are the terms normally used for security used to safeguard the supply chain (performance) from current and future displacements or antagonistic threats. According to Closs and McGarrell (2004), there are three reasons behind the increase in supply chain security interest: first, the globalization of world trade which depends on and is generated by the free flow of people, goods, and information; second, increasing demands from businesses for efficient supply chain operations; and third, increasing threats of terrorist attacks. These factors can be described as illegal and antagonistic threats, of which terrorists are one type. Therefore, supply chain security management can be defined as “the application of policies, procedures, and technology to protect supply chain assets from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain” (Closs et al, 2004). On the other hand, transport security is defined as, “the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems and workers against intentional unlawful acts” (EU, 2003). The much sought-after collateral benefit of implementing security features to prevent or deter the risk for antagonistic threats is higher supply chain efficiency. It is important to remember that “social and technological changes produce new crime opportunities” (Felson et al, 1998). These new opportunities may or may not be exploited by potential perpetrators and the potential new technological may or may not increase non-antagonistic risks. The pursuit of collateral benefit from supply chain security features is addressed in papers C, D, E, G, and H.

Supply chain performance - crime displacement – opportunity:

The goal for organisations involved in a supply chain is to provide the ultimate customer with the right product at the right time and place. The supply chain performance depends on the efficient movement of objects (products, cargo carriers, etc.) that can be threatened through different opportunities. Changes in both opportunities may lead to a displacement of the threats. If the potential risk for disturbance or threat to the supply chain performance is considered too high in a certain logistics setup or product flow, then the design of the system should be altered to reach an acceptable level of mix between constraints and risk for disturbance. This is the goal for risk management thinking/processes/theories used in the context of supply chains. The three corners of the antagonistic threat triangle show the handling of antagonistic threats to logistics is mainly a balance between supply chain performance and reducing opportunities while avoiding potential crime displacement.
6. Discussion

The results of the studies are stated in respective papers and related to the four research questions presented in Chapter 5. This chapter discusses the results in terms of theoretical and practical contributions. The problem with antagonistic threats (and other types of risk) is nothing new in the transport business. Risks have long been a factor in all business processes and will still be in the future. The interest and attention given to risk has changed during history, but all actors/stakeholders/organisations will strive for a reasonable risk exposure. The handling, management, and prevention of these threats and risks in the global flow of products have developed throughout centuries with a main focus on international relationships and conventions and enlargement of the insurance business.

The optimize principle in microeconomics and the risk assessment strategy aim to provide the parties involved with an organisational internal profit/risk/cost optimum. The extension of the guiding principle is that if the risks are handled within the free market, regardless of organisational motives, it will benefit society as a whole (Smith, 1776). The results presented in thesis clearly demonstrate that the whole system for handling antagonistic threats works, although maybe not in an optimal way. The pursuit of an internal profit/risk/cost optimum gives the risk market a semi-flexible behaviour or certain stickiness (Keynes, 1936). However, within this general way to handle threats and risks, there are winners and losers or more successful and less successful actors that handle their part of the total supply chain risk or reach their internal profit/risk/cost optimum. This general risk handling is at its best expressed by Juttner (2003) in Figure 22:

Figure 22: Supply chain risk management — basic Constructs (Juttner et al., 2003)

Figure 22 lacks the different actors involved in a supply chain and the differences and misalignment in supply chain risk management strategies and objectives. The result in Paper B indicates that the will to collaborate is less to share risks than to share earnings (even if actors are unwilling to share earnings). This means simply that in a business relationship both must parties gain by continuing the collaboration. By separating the risk sources from the consequences (different actors/stakeholders experience the risk/consequences differently), the risk is redistributed between the actors within the supply chain. This view becomes more credible as the description of the antagonistic threat becomes wicked. Rosenhead’s (1996) criteria for
wicked problem categorization give an excellent description of why it is difficult to achieve optimum risk/gain alignment in supply chains.

Accommodate multiple alternative perspectives: Each actor can model their involvement and the risk exposure that affects their own profit/risk optimisation by using different viewpoints or seeing the risk through the eyes of the colleagues in the supply chain or transport network. The actors and stakeholders need to understand and constantly share alternative perspectives or views. The results of papers B, C, D, and H indicate that this is difficult to accomplish because each stakeholder/actor acts according the central principle in microeconomics, “They do the best they can given their objectives and the constraints they face” (Mankiw, 1997) The optimize principle and the risk assessment strategy aims to fulfil Mankiw’s (1992) statement that an internal profit/risk cost optimum and each stakeholder optimum may or may not restrain another stakeholder’s optimum.

Function through group interaction and iteration: The management needs to be carried out as a group and all measures need to be readdressed within a certain time. Therefore, the continuous improvement methodology from quality management systems such as ISO is useful. The result in Paper A indicates that a common sense attitude toward parts of the antagonistic threat problem may contribute to a limitation of the interactions within the transport network.

Generate ownership through transparency: In order to facilitate collaboration and cooperation in these issues, actors and stakeholders should be transparent. This element in achieving optimum risk/gain alignment may be the hardest. It is discussed in all eight appended papers in different ways. Several obstacles are found, but few conclusions point toward a greater supply chain transparency with regard to antagonistic threat solutions.

Facilitate a representation of the solution space: The different solutions need to be presented as simply as possible to facilitate collaboration. It is in this perspective that the implementation of supply chain security programmes can be understood, but as indicated in papers B, C, and H, the implementation itself is trouble.

Focus on relationships between alternatives rather than continuous variables: The normative view of logistics as a continuous process (a.k.a., supply chain perspective) needs to be modified when managing antagonistic threats because the relationship between alternative strategies provides a better resilience in the supply chain.

Concentrate on possibility rather that probability: The risks for antagonistic threats have a lower probability than process failures (Chapter 1.1), but the consequences for the flow of products may be larger and transmitted through the chain. Focusing on the possible risks (probability and consequence together) can help develop a better strategy.

Therefore, the new problem of non-economically driven antagonistic threats toward the transport network requires a different distribution of the total supply chain risks. This does not necessarily lead to a change of risk mitigation strategies, only a different outcome. Paper H addresses this change in part of the global transport network - the ports. The results of this paper indicate that even though the ISPS-code was designed to address the terrorist threat through collateral benefits in theft reduction, it still lacks a model for distributing the costs of implementation. The fear of non-economically driven antagonistic threats has caused the creation of different supply chain security programmes. The effects on different stakeholders in the transport network are addressed in Paper C.
6.1. Results and contribution

The economically driven antagonistic threats are subject to the supply and demand forces of the gray market, while non-economically driven antagonistic threats are linked to political/ideological/religious issues. These driving forces, along with such opportunities as the unique combination of object, place, time, method, and security (or lack of), contribute to the risks and uncertainty in supply and transport chains. The characteristics of antagonistic threats against the transport network can be described with a few guiding principles that also describe the behaviour of the system. Therefore, understanding the characteristics of antagonistic threats is based on subjectivity and paradoxes instead of objectivity and rationality in the interaction between actors/elements/stakeholders. The general elements are illustrated in Figure 23:

![Figure 23: Antagonist threats against the transport network](image)

Today, managing antagonistic threats uses two different main strategies/methods—risk prevention and transfer. The two different strategies address the wicked problem of antagonistic threats differently and therefore complement each other instead. Risk prevention aims primarily to reduce the threat by addressing the probability and possibility for a certain type of threat. The prevention strategy is also valid for the consequence side of risk because the mitigation method refers to the possibility to withstand risk. The risk transfer strategy is only found on the consequence side in Figure 23 because it moves the risk through contractual agreements and insurances policies. The risk reduction strategy is based on the right management approach, correct usage of technology, and the re-engineering of operational processes.
They are equally important and it is the interaction between them that alters the opportunities for antagonistic threats in the eyes of the perpetrator.

After the terrorist attack on the World Trade Center in 2001, authorities launched several logistics security programmes that target different aspects of the physical supply/transport chain infrastructure as well as the relationship between authorities and logistics operations such as cross-border activities. The cost for implementing these programmes alters the current collaboration models with regard to risk and profit sharing within the supply chain. The risks for antagonist threats depend on the local environment, and security programmes advocate up to three different security levels to solve the problem. Therefore, the security level is adjusted toward the security programmes instead of the local threat assessment. This could mean the security cost is higher than necessary, but a standardisation of security within the supply/transport chain may result in better collaboration.

A holistic approach is needed to reduce the total risk for a supply chain, its processes, and stakeholders. The holistic approach also emphasizes the need for contextual understanding or investigating the problem’s environment. Managing antagonistic threats with a holistic approach requires leadership from all levels in an organisation to develop and implement procedures and routines and, more importantly, to amplify the human side of security. The leadership aspect involves coordination and collaboration on security and insurance coverage. Excellent security also requires physical obstructions that can contribute to logistics efficiency and prevent antagonistic threats. Smart use of information can separate legal shipments from illegal ones. This information should cover everything from the product itself to stakeholders and the freight route. This produces vast amounts of information and requires a smart filtration of information to find the illegal shipments/products/actors.

Regardless of the extent and nature of the threat toward a supply chain, the big challenge of antagonistic threats is to balance the cost of the problem against the cost of preventing it. This makes the ROI-issue or cost/benefit tradeoff the centre of preventive discussions and also provides an understanding of why collaboration between actors and stakeholders is so hard to establish.

6.1.1. Theoretical contribution

The theoretical contribution this thesis aims to provide is the use of theories from criminology to model and describe antagonistic threats toward the transport network. As demonstrated in Chapter 3.5, there is a research gap in the topic of supply chain risk management to model and include antagonistic threats in the general risk discussion. This thesis also indicates that the risk for antagonistic threats may not be the greatest threat toward supply chain performance, but nevertheless the consequences may be grave if the stakeholders are reluctant to collaborate to reduce the total risk for antagonistic threats. The assertion of antagonistic threats as a wicked problem demonstrates the need for contextual understanding to describe and understand the problem itself.

The reasons behind mentioning terrorism in several supply chain risk papers maybe threefold. First, Sheffi (2001) clearly points out the effects of the WTC terrorist attacks on the global flow of goods. The effect may be indirect, but it was devastating. This event along with non-antagonistic events such as Hurricane Katrina and other natural disasters demonstrated their power to disrupt or cause uncertainty in supply chains (Elliott, 2005; Peck et al., 2002). Second, terrorism conducts fund raising through criminal activities (Hardouin et al., 2006), which
leads to that terrorism represents all antagonistic threats. Third, the tools and strategies for handling antagonistic threats are partly governmental (police and justice system) and partly consequence handling (insurance businesses, conventions and business contingency).

Regardless of the reasons for excluding criminal activities except terrorism in general threats (Chapter 3.5) against the supply chain, the criminal problems are there (Chapter 1.1) and need to be understood. The three elements of crime are equally good to describe terrorism and other types of crime. The key difference is the perpetrator’s decision process and the desired outcome. This thesis shall be seen as a first attempt to bridge this gap in the logistics research.

The theoretical model presented in this thesis, the antagonistic threat triangle, enriches the research area of supply chain risk management with a nuanced and versatile theoretical model for future theoretical use.

6.1.2. Practical contribution

The practical contribution from this thesis is twofold. First, the common sense attitude toward the antagonistic threats and liability focusing cooperation between stakeholders has a limited reliability to reduce the total risk. The cooperation between actors and stakeholders needs to address the issue beyond organisational boundaries, both up- and downstream. The common sense feeling regarding the perpetrator’s modus operandi may reduce the implemented security or at least result in implementation of the wrong features.

6.2. Generalisation

The idea of making general claims has traditionally been a vital part of logistics research (Aastrup et al., 2008). The tradition forms of generalisation are either statistical generalisations (Yin, 1994) or nomothetic/deductive reasoning (Sayer, 2000) with strong correlation to the actual problem. The generalisation in thesis is based on deductive reasoning because of the definition of antagonistic threats as a wicked problem and the lack of statistics. This chapter contains the contextual close deductive reasoning that provides a generalisation of the results presented in this thesis.

To achieve high overall supply chain performance, processes and activities should be scheduled and managed to obtain cost efficiency and short lead-times. In the transport network this is realized by the extended use of time-windows. These windows are scheduled according to the needs or demands from the terminal, warehouse, or factory’s internal activity, or in other words, the demands from the receiver and not the forwarder or the consignor. This makes the network predictable for the actors involved, including the potential perpetrator. This predictability plays an important role in potential crimes within the network. The need from the supply chain for scheduling transport activities also provides crime opportunities, according to Cohen and Felson’s (1979) theory of routine activities perspective. The routine activities perspective in criminology states that the normal movement of the potential perpetrator and the supposed victim plays a significant role in potential crimes. The rigid scheduling in the transport network provides an excellent breeding ground for repeating crime opportunities.

The potential perpetrator who acts from a rational choice perspective will use a personalized decision process about the potential crime based on the relationship between the benefits of the crime and the troubles and risks it brings. Therefore, the creation and usage of antagonistic threats is also a subject for a benefit/trouble-risk decision process from the potential perpe-
Transport security aims to alter the outcome from the potential perpetrator’s decision process regarding the usage of an antagonistic gateway.

This risk for antagonistic threats in a supply chain risk context can be considered a part of the environmental risk. In this case, the environment is the geographical area or pipeline through which the network conducts the transport. This geographical pipeline can, depending on mobility, be under threat from numerous potential perpetrators. As the perpetrators become more professional, they will also be able to use the weak spots in the transport network within their mobility and ability.

The perpetrator’s decision process is important to understanding the use of antagonistic threats in the transport network. In other words, countermeasures should be based on an understanding of this decision process or the antagonistic dynamics of potential perpetrators. The difference in perpetrator context is vital for applying the right type of transport preventative countermeasures. Security in the transport network against these types of antagonistic threats aims to alter the contextual perception of the network and reduce the problem of antagonistic threats.

6.3. Generalisation of managing the risk of antagonistic threats

Managing antagonistic threats is not a unique feature for actors in the transport network or even in the global supply chain; it is something every organisation needs to be prepared to do. The big difference is the context in which the antagonistic threat is described. This thesis focuses on the context of global transport. The results and content are closely linked to the world of logistics, but the tools and strategies may work in other contexts if adjusted to the new context. The general model presented in this thesis is demonstrated in Figure 23 below.

![Figure 24: General model for managing antagonistic threats](image-url)
The security side of any antagonistic threat normally refers to the preventing a threat, while the consequences likewise are considered the insurance sphere. This simplification may cause problems if a certain strategy requires an adequate solution for the actors/stakeholders. This chapter contains specific suggestions and ideas of how to manage the risk for antagonistic threats toward the transport network, written in a way that is easily adjusted and adapted to other antagonistic contexts. Chapter 6.3.4 is written to understand the relationship between authorities and businesses with regard to antagonistic threat problems.

6.3.1. Perpetrator and threat opportunity

The most important thing to remember with crime opportunities is that an opportunity alone does not explain why a crime occurs. A crime needs a motivated perpetrator and an opportunity to occur (Clarke et al., 2003). The theory of crime opportunity also refers to the fourth principle of microeconomics (Mankiw, 1997) - people respond to incentives - and the degree of opportunity or incentive necessary depend on the individual. Antagonistic threats depend on motivated perpetrators, their will to accomplish the threat, and their desired outcome. However, it is still possible to classify the perpetrators into the main groups of economically driven and non-economically driven and then further divide the groups by potential targets (objects).

Crime opportunities depend on everyday movements (Clarke et al., 2003). This can be re-stated as crime opportunities depend on routines or predictability within certain boundaries, implying that system predictability or routine provides crime opportunities. The predictability can be with regard to location, time, procedures, and personnel, or routines that can be exploited by motivated perpetrators. Antagonistic threats opportunities are not the same for all potential perpetrators - each individual perpetrator subjectively estimates each individual opportunity and decides how to act in that particular situation.

The infrastructure of the transport network is, in the short term, fixed and completely predictable. The movement of resources between terminals, factories, and other nodes also is predictable to a large extent. The flow of material varies to a higher extent but depends on the actors within the supply chain. Therefore it is possible to predict the flow of goods to some extent.

A “hot product” is a product that is CRAVED: concealable, removable, available, valuable, enjoyable, and disposable (Clarke, 1999). This term is used usually in a retail context, but it is useful to anticipate a higher exposure of certain products for criminal purposes. In terms of terrorist attacks, the hot product can be distinguished as a product (target) with high political, ideological, or emotional value to the perpetrator or the public.

6.3.2. Mitigation of antagonistic threats

The mitigation of antagonistic threats refers to strategies to reduce the impact. Mitigation ranges from contractual work (transfer strategy) to higher inventory levels, multiple suppliers (Sinha et al., 2004; Sheffi, 2001) and preventive measures. In practices are these three mitigation methods used together to strengthen each other. The prevention of incidents are traditionally closely linked to the definition of security as a show of force (Borodzicz, 2005) which leads to that security work becomes symbolised with uniformed guards and normal police duties. In order to include impact reduction in the term security is the second definition, freedom from danger, better to use. This definition embraces all things that allow the organisation
to act and carry out the business “free from danger” (Borodzicz, 2005). This leads to that prevention and investigation of crimes (all types) are included in security and therefore are under the subject of a mitigation strategy. Successful mitigation depends primarily on the right combination of leadership, tools, and equipment.

6.3.3. Transfer of antagonistic threats

The mitigation of antagonistic threats refers to strategies to transfer the economic impact to another organisation/company. The basic idea is that by transferring the risk to someone else through different types of contracts, it reduces personal risk substantially. The contractual agreements are divided into two different categories - insurance policies and non-insurance contractual agreements between two organisations. Good risk transfer strategy is composed normally of both types of risk transfer.

Transfer of risk by usage of insurance: The insurance principle prescribes that the insurance company takes over the economic impact if something happens that is covered by the insurance contract. Therefore, the risk of this event needs to be rather easy to identify, classify, and determine for the insurance company to estimate the cost related to the risk and determine the insurance premium. This premium is also accompanied by an insurance excess, giving the potential insurance buyer three components to consider: the terms, premium, and excess of specific insurance. The incentive for each individual insurance buyer is the central issue, and in extension, also the potential reduction of a potential loss (Keller, 2003).

Today special insurance polices exist for everything from cargo damage and machinery breakdown to terrorism, war, and general consequence liability. Typically, all insist on special events to be considered valid for a certain incident. Sometimes the terms are so specific that different types of insurance are valid depending on the cause of the incident. One of the best examples is the often-conflicting terms in terrorism contra war insurance. If there is a recognized government behind the incident, then war insurance is valid, but if the incident is caused by someone else, it is the terrorism insurance policy that covers the economic impact. This also depends on the different terms that each insurance company has in their product.

Transfer of risk by usage of business power: This risk transfer strategy is commonly used between contractual partners, but is rarely mentioned because it opposes the belief that everybody wants to collaborate fairly and for the greater good (Mears-Young et al., 1997; Gentry, 1996; Lambert et al., 1998; Yu et al., 2001). The general idea of this risk transfer strategy is to use the business power of size, information advantage, or control over a critical asset (Cox et al., 1992) so the business partner can obtain a share of the business risk as a part of the contractual agreement (see chapters 2.10.2 and 2.10.3). Papers B and D touch upon this subject.

6.3.4. Compliance with logistics security programmes

The compliance with these different logistics security programmes is based on different reasons. The compliance with business logistics security programmes such as like TAPAs is based on customer requirements because these programmes focus on theft prevention. The governmental logistics security programmes such as AEO, C-TPAT, CSI, etc., focus more on preventing terrorist activities. These programmes also contain a disadvantage for the organisation if it does not comply. Therefore, the governmental logistics security programmes have a higher likelihood of compliance because the need for compliance is not based on a risk assessment of the potential causes and impacts for antagonistic threats but rather on a general business assessment. This difference is supported by the results presented in papers C and H. Regardless of the reason for compliance, the governmental logistics security programmes may
result in collateral benefits such as lower cost for theft and better working conditions for employees (Paper H). It is still to be demonstrated that the terrorism prevention logistics security programmes actually reduce the risk for non-economically driven antagonistic threats. The compliance with different logistics or supply chain security programmes needs to be addressed more in the future due to their novelty and effects on the global transport network. Chapter 7.2 addresses this idea.

6.3.5. Cargo crime as a production method

Logistics are, according to Christopher (2005), “the process of strategically managing the procurement, movement and storage of material, parts and finished inventory (and the related information flow) through the organization and its marketing channels in such a way that current and future profitability are maximized through the cost-effective fulfilment of orders”. Better business deals are the practical way to maximize profitability and, according to Naylor (2004), this drive and the general globalization trend led to the embedment of illegal actions within legal markets (cf. Antonopoulos, 2007).

Cargo theft is unique among contraband supply methods because it has the lowest cost structure - lower than in smuggling, counterfeiting, or product piracy. Conversely, it offers organized crime groups the highest potential profit margins. By relying on cargo theft to obtain its contraband supplies, an organized crime group could gain competitive advantage against rivals employing smuggling, counterfeiting, or product piracy (FIA, 2001). Considering the cost side for supply chains and its logistics and comparing legal and illegal supply chains from a cargo theft perspective, it is clear that they both have costs. From the Point of Theft (POT) to the Point of Sale (POS), the cost (actual cost + risk premium) for illegal supply chains is higher. The higher illegal supply chain cost is due to the fact that the illegal system must avoid discovery from authorities (Ekwall, 2009 - b). The value of the stolen product is determined by the market for the legal products (cf. Smith, 1776; cf. Mankiw, 1992), and therefore the trade with illegal products is analysed with the general principles of microeconomics (Chapter 2.2.1).

In order to fully understand the cargo crime context and the wicked problem of antagonistic threats, cargo crime shall be considered an alternative supply method with other benefits and drawbacks than the legal supply chain, in addition to the fact that cargo crime is a crime (with adherent features). This understanding can be illustrated with a cost comparison example between a legal supply chain and two types of cargo crime supply chains.

If we consider the value of the products delivered by legal or illegal supply chains and the size of the components, we can understand the cost-value-structure of both systems. Legal supply chains include the cost of the product (development, production, and marketing, etc.) and logistics to get the products to the POS. In addition, there are authority demands regarding taxes and VATs, and the actors have a desired margin of profit for their participation. Illegal supply chains include the cost for the theft or counterfeiting production and logistics to get the product to the POS, and then the rest is the revenue only. To understand the differences between the two major types of illegal supply chains, it is useful to plot a risk cost to make it clear which type has the highest risk for detection (cf. BRÅ, 2007). The customer price of an illegal product is usually lower than the legal price, but the revenue is in all cases higher because of the considerably lower cost structure. An example of this cost comparison is illustrated in Figure 25.
**Figure 25: Costs comparison example between legal business and cargo crimes**

This is only a general comparison and may fluctuate due to the demand and supply for a certain product in a certain place and at a certain time (cf. Mankiw, 1992). The interesting part of the cost comparison in Figure 25 is that with the background in Christopher’s definition of logistics (2005) is it easy to understand and foresee Naylor’s statement (2004) about the embedment of illegal actions within legal markets. The embedment solves two problems at the same time. First, it ensures the current and future profitability are maximized within an organisation through the cost-effective fulfilment of orders. Second, it reduces the risk for discovery by the authorities or other stakeholders that are affected negatively by the embedment (Ekwall, 2009 - b). Christopher’s definition (2005) does not state that illegal actions are allowed or desirable, only that maximized profitability is the goal and as a consequence, cargo crime can be understood as an alternative production method.

### 6.3.6. Terrorist threat toward logistics operations

The World Trade Center attack in 2001 changed the world and with it the conditions for logistics worldwide. The aftermath of the terrorist attacks clearly indicated that in case of a terrorist attack, will logistics operations suffer. This indirectness or lack of distinct causal relations between cause and consequence for terrorist attacks (from the non-perpetrator point-of-view) and logistics operations makes the antagonistic threat a wicked problem. This can be demonstrated in two steps, target and consequence.

**The Target:**

Terrorism is defined by TE-SAT (Europol, 2007) as, “not an ideology or movement, but a tactic or a method for attaining political goals. This definition clearly states that terrorism is a driven by non-economic issues and therefore the targets also are selected to maximise the non-economic penetration from the perpetrator’s point-of-view. Approximately half of the terrorist attacks during 2006 (~46 percent) was directed against representatives for states and

<table>
<thead>
<tr>
<th>Legal products</th>
<th>Counterfeit products</th>
<th>Stolen products</th>
</tr>
</thead>
<tbody>
<tr>
<td>VAT</td>
<td>Pricing to lure customers of the legality of the product</td>
<td>Pricing to lure customers of the legality of the product</td>
</tr>
<tr>
<td>Margin of profit</td>
<td>Revenue</td>
<td>Revenue</td>
</tr>
<tr>
<td>Marketing cost</td>
<td>Risk premium</td>
<td>Risk premium</td>
</tr>
<tr>
<td>Logistics cost</td>
<td>Logistics cost</td>
<td>Logistics cost</td>
</tr>
<tr>
<td>Production cost</td>
<td>Production cost</td>
<td>Theft cost</td>
</tr>
<tr>
<td>Development cost</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legal business

Cargo crimes
governments while 4 percent was aimed directly against transports and an additional 4 percent against general business (Chapter 1.1.5).

For terrorist threats, it is useful to refer to transferred and perceived threatening pictures (cf. Sjöberg, 2008). The perceived or actual marketing strategies which link a company or organisation with certain values/states/advocates will affect the risks for terrorist threats to the organisation/business/market position. The key issue in this conclusion is that the perceived relationship between a company/organisation and values/states/advocates is made by the potential perpetrators. Therefore it is important for a holistic threats assessment to include and consider these different relationships between an organisation and different values/states/advocates with regard to direct and more important indirect connections.

Historically, terrorist groups and organisations have been closely related to a certain geographical area and executed in that area. This is a valid statement for terrorist organisations such as IRA and the Basque separatist movement, even if both have conducted attacks outside their fighting area but within their targets (e.g., in UK but outside Northern Ireland, and in Spain but outside the Basque province). Those types of organisations only constitute a threat if the operations are carried out in that area and if the logistics operation possesses any real or symbolic value for the terrorist organisations. The strong relationship between different terrorist groups and geographical area may be reduced when referring to international terrorist organisations such as Al-Qaeda, but the targets should still possess a symbolic value for the terrorist organisations, even if the value is public fear.

*The Consequence:*

Whether the supply chain was directly involved or targeted by a terrorist attack may mean the supply disturbance will affect an organisation in different ways. The direct management of these indirect effects can be separated into two different main methods - insurance and logistics security programmes. The global market for terrorist insurance works in the same way as the global market for liability insurance. Terrorist insurance shall be seen as a complement to other types of insurance policies, which normally exclude terrorist attacks from their coverage. The second type of managing this problem is to comply with the different international logistics security programmes that focus on preventing terrorists from abusing the global transport network for attack or preparation for attacks. Regardless of which method is used in an organisation, they will work only with a low causal relation to the actual threat from terrorists.
7. Conclusions and future research

This chapter contains the main conclusions of this thesis and presented future research topics and specific research papers.

7.1. Conclusions

A contextual understanding of antagonistic threats toward the transport network is important to be able to successfully manage them. The different types of threats (economically and non-economically driven) need to be understood and managed differently. The simplistic categorisation of antagonistic threats is only valid in theory because perpetrators are in reality motivated by several different factors in an individual manner, which can be described as partly economically and partly non-economically driven (see chapters 1.1.2; 1.1.5; 2.10). It is important to recognize and understand that the perpetrators and their reasons that are the key in preventing each antagonistic threat. The categorisation of perpetrators leads to a better understanding of the effects that antagonistic threats have on business and how they can be managed more effectively. The antagonistic threat triangle (Figure 15) is an illustration of elements, events, and relationships within the supply chain risk context that explains and simplifies the understanding of antagonistic threats.

The management of antagonistic threats using the risk management perspective is separated into two pre-event and post-event measures. The pre-event stops the event from occurring or reduces the likelihood of a certain event (preventive measures etc.). The post-event measures attempt to reduce the operational impact and economic consequences (business contingency and insurance policies etc.). Therefore, using logistics terms, the system needs to be robust and resilient. It should be robust enough to handle automatically small risks with high likelihood and low impact so the performance of the system is never threatened. The system also needs resilience to adapt, improvise, and overcome any disturbance greater than the robustness of the system can handle. The system’s robustness and resilience can constitute of the full range of preventive, mitigating, and transfer tools and methods. From a business perspective, the multiple stakeholders’ judgment and interpretation of the problem with antagonistic threats are so different that a complete definition of the exact problem and a clear end-point is practically impossible to obtain. Regardless of which perspective is chosen to analyse the problem, the same basic set of tools and methods need to be adapted in practical use to the actors’ needs and wants for managing antagonistic threats.

7.1.1. Proportions and patterns of the problem

The traditional approach to risk management uses statistical methods to establish a risk cost for each problem. This leaves little room for alternative perspectives, but if the relationship between cause and consequence is strong and linear is there little need for different ways to address each problem. As demonstrated through the use of the cargo theft cost calculation in Appendix D, it is possible to state that the annual risk cost for cargo theft in Sweden is fairly large, but represents only a fraction. The same picture is found in Chapter 1.1.7 where the statistics from a LSP with regard the FFL states that cargo damages represent roughly 90 percent of the claims and cost. The same picture can be found by comparing the annual reported number of different crimes in Sweden. According to SSLF (Swedish Association for Provision Grocer's Shop Owners), it is estimated that nearly 1,000 stores or 14 percent will be
robbed in 2008 (SecurityUser, 2008). The same frequency for road transports in Sweden would involve 5,307,960 attacks, compared to 2377 reported in Sweden in 2007. Based on statistics, it is reasonable to state that cargo thefts are not a major threat when compared to other crimes. Nevertheless, it is a costly and wicked problem that needs attention.

This statistics do not provide a full image of the problem with claims because the fragmentation of the transport business makes it possible to dilute the claims, costs, and amount for the actors using contractual agreements and insurance policies. The problem with non-economically driven antagonistic threats is in pure numbers - they are a very small ratio in comparison with the business as a whole or even as a risk cost. The big difference is that the impact of non-economically driven antagonistic threats propagates further and faster within the supply chain, generating more uncertainty and higher impact costs than economically driven antagonistic threats. Even if the risk cost (probability and impact) are lower for non-economically driven antagonistic threats than economically driven threats, they need to be managed as well (cf. Ekenberg, 2001). Therefore, the problem with antagonistic threats is better described as possible rather than probable.

In linear terms, the problem with antagonistic threats occurs when the capability of the preventive measures is lower than the capability of the perpetrator. This is a simplification of the relationship between perpetrator and guardian (see chapter 1.1.1, elements of crime). This relationship is dynamic and closely linked to local conditions. Therefore the proportion and pattern of antagonistic threats are also dynamic and closely linked to local conditions (Paper A).

7.1.2. Understanding of the problem

The understanding of the problem with antagonistic threats toward logistics operations can be divided into two approaches for theoretical reasons. The first approach is the supply chain internal viewpoint. This step includes only controllable features in the supply chain. This viewpoint sees the supply chain as a stand-alone system under threat from hostile external forces (a.k.a., the potential perpetrators). The border between internal and external is very difficult to establish, but normally is defined by measures of direct control from one or several actors in the system. The second approach is the extended or holistic approach, which emphasizes the interdependency between the supply chain and surrounding societies/environments. The first approach is normally and correctly used in logistics research, but the extended or holistic approach is more useful to fully understand the problem of antagonistic threats. In this approach, the perpetrator is included in the research, and instead of being seen as a mythical and hostile external threat, it is understood as an unwanted and uncontrollable actor/stakeholder in the supply chain. The antagonistic threat triangle (Figure 15) and the antagonist threats against the transport network (Figure 3) represent models that use the holistic approach to describe the elements of antagonistic threats.

The occurrence of antagonistic threats toward supply chains and transport network is not a new problem. Throughout history there have been innumerable examples of different modus operandi (methods), targets, preventive measures, and perpetrator characteristics. Common for all examples are the three elements of crime and the wicked problem description. The occurrence of antagonistic threats, whether the target is the global transport network or not, is mainly a social problem which always is related distinctly to the wider context. Therefore, different organisational boundaries demarcate only the direct relation to the problem while the indirect problems are related to the relationship between an organisation and its environ-
ment/society. Managing these problems fulfils Rittel’s (1973) statement regarding the nature of a wicked problem, “any solution, after being implemented, will generate waves of consequences over an extended – virtually an unbounded – period of time. The next day’s consequences of the solution may yield utterly undesirable repercussion. In practical terms, the actors and stakeholders that try to manage antagonistic threats need to rethink their methods/strategies/attitude every day because of changes caused by the parties involved or the surrounding environment. Stakeholders and actors may be using similar methods/tools to manage antagonistic threats, but their differences will change the effects and consequences of these preventive measures.

Making the problem of antagonistic threats even more wicked is the fact that the parties involved (or their human representatives) have different risk apprehensions. Two similar or even exact actors may interpret or estimate their risk/explanation for these problems differently. The understanding of different risk apprehensions is essential to understand the current development of the logistics security programmes aimed at reducing the risk for terrorists adding bombs into a shipment and threatening key infrastructure while causing massive flow disruptions. The likelihood of a terrorist attack using that modus operandi is low (Chapter 1.1.5) while the potential impact is grave. Therefore, the apprehension/perceived risk is huge even if the likelihood is so low that the actual risk cost is lower than a regular cargo theft. It is human risk apprehension that lures them to perceive terrorists as a major threat instead of the actual risk for an attack. It is important to remember that a terrorist’s target is not the global flow of goods, but public fear. This fear can induce such psychological effects that cause public communities to significantly alter the economic development of a country (Lin et al., 2006). This is the understood effect from terrorists instead of a cargo theft mainly driven by economical issues (cf. Christopher, 2005; cf. Smith, 1776; cf. Mankiw, 1997).

### 7.1.3. Managing the problem

A holistic approach is needed to reduce the total risk for a supply chain, its processes, and stakeholders. The holistic approach also emphasises the need for contextual understanding or investigating the problem’s environment. Managing antagonistic threats with a holistic approach requires leadership from all levels in each organisation to develop and implement procedures and routines and to amplify the human side of security. The leadership aspect involves coordination and collaboration with regard to security and insurance coverage. Excellent security also requires physical obstructing artifacts that can contribute to logistics efficiency and prevent antagonistic threats. The security is based on the right management approach, correct usage of technology, and the re-engineering of operational processes. They are equally important and it is the interaction between them that alters the opportunities for antagonistic threats in the eyes of the perpetrator. The security effort aims primarily to reduce the likelihood of an antagonistic threat while risk transfer strategy handles the consequences of an incident. If the transfer strategy is not applicable, the different mitigation tools are the last line of defense for an organization.

After the terrorist attack in the World Trade Center in 2001, authorities launched several different logistics security programmes to target different aspects of the physical supply/transport chain infrastructure as well as the relationship between authorities and logistics operations such as cross-border activities. The cost for implementing these programmes alters the current collaboration models with regards to risk and profit sharing within the supply chain. The risks for antagonist threats depend on the local environment and each individual potential perpetrator’s decision process.
7.2. Future research

This thesis is the first attempt to include theories from criminology into the scientific field of logistics and supply chain management. This inter-linkage or mutual adjustment of several theories inevitably leads to many new research ideas and paper suggestions. The pursuit to develop or create new theoretical models in order to make general claims has traditionally been a vital part of logistics research (Aastrup et al., 2008). The model of the antagonistic threat triangle presented in this thesis would certainly benefit from further development and adjustment. Beyond that, several different research ideas can be presented in this chapter which are either closely linked to the context of antagonistic threats or found in the intersection between different theories from either criminology or supply chain management. These ideas can be presented as either general ideas or concrete paper suggestions.

General ideas for future research areas

This thesis takes a top-down perspective on the problem with antagonistic threats in a transport network. This means basically that the logistics business has been simplified into a transport network in the form of a system with complex behaviour. Each different actor or stakeholder can address the problem with antagonistic threats differently and therefore affect the whole system’s preventive actions.

The number of papers published addressing the subject of supply chain risk management has increased in recent years (Brindley, 2005). This indicates that risk questions in a supply chain context are becoming more interesting for scientists and businesses. The same development can be seen in the subject of supply chain security. This thesis separates statistical from contextual risk management approaches caused by the threat. Will this relationship between risk management approaches be the same in a supply chain context?

During the work with papers D, C, F, G, the problem with insiders appeared. An inside position or inside information about a certain shipment or transport is useful for a potential perpetrator. The literature has different opinions about the severity of the fear of insiders. Some authors consider insiders to be involved in approximately 60 percent of all losses (Tryon et al., 1997), while others claim there are no reliable figures (Muir, 1996). Twenty-three of 30 organisations in Paper C believed that the insider problem was not overrated. This is interesting when compared to the fact that most countermeasures are implemented to reduce external theft (Beck, 2002). If the inside problem is as serious as the stakeholders claim in Paper C, how can preventive measures be introduced into the transport network to address the problem with internal thieves?

The implementation of supply chain security programmes has so far mainly occurred in the old western countries in North America and in Europe. This shall be compared with the statistics of terrorist attacks presented in chapter 1.1.5. The actual occurrence of terrorism and the implementation seems to be asymmetric but if the development and implementation of supply chain security programmes is understood as dependent on asymmetric risk perception based on the very same fear that the terrorists primarily use as the way to influence the political development. The implementation of supply chain security programmes maybe requires a stabil and powerful government acting with internal economies that minimize the occurrence of different informal trades?
Suggestion for future papers

The theories presented in the framework in this thesis lead to eight new suggestions for papers. These eight suggested papers address different aspects of the problem with antagonistic threats toward the transport network. Competing interests and the lack of universal solution can be illuminated in several different perspectives. The suggested papers are presented in relationship to the thesis model in Figure 26. Five of these papers have clear links to the concept of supply chains, which leads to a more distinct focus on supply chain theories and the managing of antagonistic threats.

Figure 26: Links between suggested future papers and this thesis model

**Paper I**: Since several different supply chains are present at the same time and in the same place in the transport network, the consequence of an unwanted event often becomes more complex to handle than preventing the event from happening. This acknowledgement indicates that the relationship between supply chains and transport activities would be better described with complexity theory, especially if the interactions between components are the object for the research.

**Paper II**: The occurrence of criminal background check within the field of logistics security is an increasing security requirement, but this needs more research in order to clarify the content, purpose, and effects of these criminal background checks. It needs to be clarified whether these background checks lead to fewer incidents (mainly theft incidents) or if the outcome is the same.
**Paper III:** The usage and design of different insurance policies in logistics operations needs more research to be better understood and put to more effective (total supply chain cost meaning) use in the future. The stipulation of the both insurance premium and adherent deductible needs to be included in this paper to use the holistic approach, which is needed to understand the total supply chain cost perspective.

**Paper IV:** The usage of Incoterms 2000 in logistics operations needs more research in order to be better understood and put to more effective (total supply chain cost meaning) use in the future. Incoterms are related more closely to the actors in the supply chain (consignor and consignee) than to the operators in the transport network, but the chosen Incoterm affects the payment, insurance, and delivery conditions fulfilled by the actors in transport network.

**Paper V:** The usage of a holistic approach in logistics research is needed to be credible when including the managing of antagonistic threats. Does this result in the involved stakeholders adopting a more holistic approach in their daily operations or is this approach only something that is valid in research? The usage of a holistic approach toward antagonistic threats clearly needs more research.

**Paper VI:** The small difference between the terms supply chain risk management and supply chain vulnerability needs definition. Several authors (Narayanan et al., 2004; Agrell et al., 2004; Chopra et al., 2000; Lee et al., 1999; Bai man et al., 2001; Ming et al., 2003; Lundin, 2008) use the term supply chain misalignments to master the dynamic in a supply chain with unnecessary vulnerability to which the actors contribute by not collaborating together to minimise the entire supply chain vulnerability. The risk clauses in the contractual agreement between actors in the supply chain needs to be linked to the different actor’s liability and reflect a reasonable risk/profit exposure for each actor. This paper should address the practical usage of supply chain alignment theories.

**Paper VII:** The movement of resources between terminals, factories, and other nodes is also predictable to a large extent. The routine activity perspective states that the predictability in infrastructure and resource movement will significantly contribute to establishing crime opportunities. The load or the flow of material varies to a higher extent but depends on the actors within the supply chain instead of actors in the transport network. The relationship between the theory of routine activity from criminology and general transport network behaviour needs to be further illustrated.

**Paper VIII:** The compliance with different logistics or supply chain security programmes needs to be addressed more in the future due to the novelty and their effects on the global transport network.
8. References


Arbnor, I. and Bjerke, B. (1997), Methodology for creating business knowledge, SAGE Publications, California.


Chong, Y. Y. (2003), ”How to achieve realistic risk management”. *Balance sheet*, Vol. 11, No. 4, pp. 44-64


EU Commission (2008), *Public Consultation in preparation of a Legal Proposal to combat counterfeit medicines for Human Use - Key Ideas for better Protection of Patients against the risk of Counterfeit Medicines*, Brussels


FIA (2001), *Contraband, organized crime and the threat to the transportation and supply chain function*. FIA International research ltd


Gammelgaard, B. (1997), ”The system approach in logistics”. In proceedings of Nofoma 1997, Copenhagen


Gearson, J. (2002), ”The nature of modern terrorism”. *The political quarterly publishing*, pp. 7-24


Holmes, J. L. (2004), ”The container security initiative: is container security a global challenge or a supply chain headache”. *Fleet Equipment*, August 1


IRU (2008), *Attacks on drivers of international heavy goods vehicles*. INTERNATIONAL ROAD TRANSPORT UNION, GENEVA


Lundin, J. (2008), *Developing a framework for describing and analyzing misalignments in the supply chain*. Department of Industrial Management and Logistics, Lund University: Lund


Robinson P. V. (2009), ”Freight crime in Europe: what happens next?”. *A presentation at ESCB 09*, Prague


Solem, O. (2003), ”Epistemology and logistics: A critical overview”. Systemic practice and action research, vol 16, no. 6, pp. 437-454


Spiegel, J. (2007), The effect of setting standards on the civil liabilities of logistic service providers. TAPA Q4, Malta


Tweddle, D. (2007), ”Logistics, security and compliance: The part to be played by authorized economic operators (AEOs) and data management”. World Customs Journal, Vol. 1, No. 2, pp 101-105


WEB:

http://www.tapaemea.com/engl/fsr.html


Appendix A - Additional publication by the author

2004


2005


2006


2007


2008

Ekwall, D. (2008), “The Displacement effect in cargo theft”. In proceedings of Nofoma, Helsinki


2009


Appendix B - List of organizations involved during the research process

The organizations listed here have all contributed in various ways to the research with information and interviews.

**Logistics Service Providers**

Cargonet
DSV
DHL Express
DHL Solutions
Frigoscandia Distribution
Green Cargo
Pan Nordic Logistics
SAS Cargo
Schenker AG
Schenker North
Swedish Post
TNT Freight Management
Tradimus Logistics
UPS North

**Insurance companies**

If
Larmtjänst
Länsförsäkringar
Trygg Hansa

**Ports and shipping companies**

Port of Gothenburg
Stena Line
Transatlantic
Viking Line

**Goods owners**

El-Giganten
Husqvarna
ICA
Åhlens
Consultants and other experts

Guard Systems
G4S Maritime & Logistic Security
Panaxia Security
Securitas Transport Aviation Security
Swedish Association of Road Haulage Companies
Swedish Defence Research Agency
SP Swedish National Testing and Research Institute
Volvo Technology
The Swedish Theft Prevention Association
Transek
Transportjuristen
University of Gothenburg
University of Lund
YourSec

Authorities

National Criminal Investigation Department
Swedish Customs
Swedish Police (districts, Västra Götaland, Jönköping, Kronoberg, Skåne, Halland)
Swedish Coast Guard
Appendix C – Glossary and Abbreviations

**AEO.** Authorized Economic Operator.

**CBP.** Customs and Boarders Protection.

**CCTV.** Closed Circuit Television.

**CIF.** Cost Insurance and Freight.

**CIP.** Carriage and Insurance Paid.

**CIM.** International Convention concerning the carriage of goods by rail.

**CRM.** Convention relative au contrat de transport international de Marchandises par route.

**CSI.** Container Security Initiative.

**CSO.** Chief Security Officer.

**C-TPAT.** Customs Trade Partnership Against Terrorism.

**EMEA.** Europe Middle East Africa.

**FAST.** Free and Secure Trade.

**FSR.** Freight Security Requirements.

**ICC.** International Chamber of Commerce.

**ICSC.** International Cargo Security Council.

**IIS.** Incident Information Service.

**IMO.** International Maritime Organization.

**ISO.** International Organization for Standardization.

**ISPS.** International Ship and Port facility Security Code.

**JIT.** Just In Time.

**LSP.** Logistics Service Provider.

**NSAB.** Nordiskt Speditörförbunds Allmänna Bestämmelser.

**OECD.** Organization of Economic Cooperation and Development.

**ROI.** Return Of Investment.
**TAPA EMEA.** Transported Asset Protection Association.

**TQM.** Total Quality Management.

**TSR.** Trucking Security Requirements.
Appendix D – Cost calculation for cargo theft in Sweden

One of the most justifiable questions regarding the wicked problem with antagonistic threats is the cost for it. Few trustworthy calculations exist and they are all more or less conjectures because even the official statistics are at best untrustworthy. This appendix presents two different and independent cost calculations for cargo theft in Sweden. These calculations shall be seen with a holistic perspective and it is only when they are used together that they contribute to the stipulating of cargo theft costs. The term cost in this appendix is difficult to use because it can represent the direct cost, the payment, or even all involved costs. This clearly contributes to the uncertainty of all calculations.

**Top-down conjecture**

The top-down conjecture uses the statistics presented in Chapter 1.1 to establish the cost. The top-down conjecture uses different percentages to narrow down the possible cost.

The total value of transported goods in Sweden: 2,093,000,000,000 SEK (SIKA, 2006)
The total amount of goods transported within the transport network: 98.5% (SCB, 2008)
The total losses during transport: 0.025-0.14% of the value (Chapter 1.1.6)
The theft ratio of the total losses during transport: ~10% (Chapter 1.1.7)

This gives that the value of stolen goods during transport in Sweden for one year is 52 – 293 million SEK.

**Bottom-up conjecture**

The bottom-up conjecture uses the statistics presented in the official Swedish police record for cargo thefts.

In 12 percent of all reports were there values on the stolen products presented. The summation of the total stated value was 12 million SEK (Nilsson, 2008). A linear conjecture of this indicates that the total value of all stolen goods is 100 million SEK for southwest Sweden. The southwest Sweden represents roughly 20% of all reports. This gives that the value of stolen goods during transport in Sweden annually is around 500 million SEK.

In the report “Attacks on drivers of international heavy goods vehicles” by IRU (2008) is the mean value €25,000 per incident (including lorries and trailers). This gives a total direct cost as around 550 million SEK.

In the report “TruckPol Annual Report 2007” by TruckPol in UK is the average loss per incident £35 214 (€47 146). The theft of truck and hi-jacks are included in this number. A correction of this gives the average loss value €18 858. A rough estimations using TruckPol’s number in Sweden gives the following numbers:

Loss value (2008): 375 million SEK
Including correction for theft of truck (2008): 616 million SEK

This indicates the annual loss value in Sweden is around 400-550 million SEK.
Cost and occurrence comparison

Relative comparisons between different types of costs are a good method to understand the size/impact for the cargo thefts on business in general.

First comparison: The costs for thefts at retailers (Swedish Trade Federation, 2007):

<table>
<thead>
<tr>
<th></th>
<th>Retail</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total cost:</td>
<td>9 billion SEK</td>
<td>400 million SEK</td>
</tr>
<tr>
<td>Loss/incident:</td>
<td>450 SEK</td>
<td>30 000 SEK (Paper C)</td>
</tr>
<tr>
<td>Number of reported crimes</td>
<td>60 000</td>
<td>2140 (Nilsson et al., 2009)</td>
</tr>
<tr>
<td>Loss ratio of turnover</td>
<td>3-3.5%</td>
<td>0.025-0.14% (chapter 1.1.6)</td>
</tr>
<tr>
<td>Solve percentage (BRÅ, 2008) (Chapter 2.11.2)</td>
<td>61%</td>
<td>2%</td>
</tr>
</tbody>
</table>

Table 21: Comparison of losses at retailers and distribution in Sweden 2007

The comparison above demonstrates that the problem with thefts is considerably larger at retailers than during distribution, but the perpetrators that attack the transports normally tend to steal for considerable higher value in each incident. The extension of this conclusion is that the perpetrators that attack the transport network are to be considered more professional (adaptable to different theft preventive measures) than the average retail store thief (see Chapter 2.11.8). A comparison between loss ration in terms of percentage of turnover clearly states that the problems in retailing is 20-140 times bigger.

Second comparison: Fuel cost road transport

The value of stolen goods is estimated to be € 6.72 per trip (EP, 2007). How big is this cost in comparison with fuel costs?

This value in diesel gives a rough estimate of 4.5-5 litres (fuel price and exchange rate 2008-10-01) and this is equal (estimated) with 10km (large trucks) and 15 km (distribution trucks) distance covered.

Discussion of the two comparisons

Both the comparisons clearly demonstrate that the estimated cost for cargo thefts are low in relation with other costs in the supply chain or for the hauler. This may explain the weak interest from the business itself to address the problem because they have bigger (more costly) problems.

Conclusions

The two different and independent cost calculations clearly indicate the difficulty of stipulating the value of stolen goods during one year in Sweden. The two calculations stipulate that the value is 350 - 550 million SEK annually. From this value is it possible to estimate the total cost for cargo theft to 4 – 7 times the value of the products. This differs greatly depending on vast amount of variables, but 4 – 7 times the value is a good conjecture. This leads to an estimated cost of 1.4 billion – 3.8 billion SEK annually. These numbers are only rough estimates and shall not be taken as absolute in any way but as cost indications for the total business.
In the report “Organised theft of commercial vehicles and their loads in the European union,” by the European Parliament, states that the value of stolen goods is € 6.72 per trip (EP, 2007). This gives the value for Sweden:

The number of road transports in Sweden in 2007 was: 37,914,000 (SCB, 2008).

This gives the value: 2.4 billion SEK.

Therefore is it believable that the total cost for cargo thefts in Sweden annually is between 1.4 billion – 4 billion SEK, with a likely peak at approximately 2.4 billion SEK, of which the direct cost (cargo value) is 200 million – 700 million SEK (peak at approximately 400 million SEK) annually.

A different expert opinion in the Swedish logistics industry considers the estimated value, 400 millions SEK annually, as reasonable, but they also remark that the estimate maybe higher than the actual value.

Reference:

BRÅ (2008), The Swedish National Council for Crime Prevention
http://www.bra.se/extra/pod/?action=pod_show&module_instance=21&id=444&statsType=170&statsCounty=La&Year=2007&type=1 (printed 2008-11-03)


IRU (2008), Attacks on drivers of international heavy goods vehicles. INTERNATIONAL ROAD TRANSPORT UNION, GENEVA


SCB (2008),
http://www.scb.se/statistik/TK/TK1007/2003M00/TK1007VFU1.xls (printed 2008-08-14)
http://www.scb.se/templates/tableOrChart____34657.asp (printed 2008-08-14)


The displacement effect in cargo theft

Daniel Ekwall
School of Engineering, University College of Borås, Borås, Sweden

Abstract

Purpose – The aim of this paper is to analyze and explain why cargo theft continues to occur in the transport network despite all implemented countermeasures.

Design/methodology/approach – The research is based on a logical deductive hypothesis using theories from several scientific fields. This hypothesis is then tested empirically. Credibility is substantiated with the use of several independent official statistical sources and verified with both open-ended qualitative interviews and a quantitative, comparative, geographically controlled survey.

Findings – Theft risk arises from different theft opportunities that will always be present in the transport network. The theory of crime displacement provides one likely explanation as to why the absolute reduction, instead of a theft pattern alteration, is very difficult to achieve. The result in this paper substantiates research results in criminology that indicate that causality in crime displacement is hard to establish.

Research limitations/implications – This research is limited by the lack of reliable information sources about criminal activities against logistics business. Secondary sources, like official crime statistics, are at best untrustworthy but more likely filled with large parts of hidden statistics.

Practical implications – The common-sense feeling about the crime displacement theory that exists in the logistics business needs to be modified. This paper maintains that the understanding of the relationship between potential perpetrators and theft preventing measures is a key issue to reduce theft problems within the transport network.

Originality/value – This paper is a step towards bringing theories from criminology into the scientific field of logistics and supply chain risk management.

Keywords Supply chain management, Theft, Risk management, Transportation

Paper type Research paper

1. Introduction

Recently, there is a significant problem with the theft of cargo worldwide. It is estimated that theft represents losses of at least US$10 billion per year in the USA and US$30 billion worldwide (Barth and White, 1998). The theft of cargo value for the EU-area is estimated to be €8.2 billion each year, which allocated on all transports, gives an average value of €6.72 per trip (EP, 2007). Gathering accurate numbers for cargo theft losses is difficult, and, in many cases, impossible, due to limited reporting by the transport industry and the lack of a national law enforcement system requiring reporting and tracking uniformity (CEMT, 2001). Despite these figures, cargo theft generally has had a low-priority status in most countries and is often perceived largely as the cost of doing business (EC, 2003).

1.1 Background

In recent years, the cargo transport process has improved mainly in the areas of logistics efficiency and documentation handling. Security within the cargo transport process, however, has not been as fortune. This deficiency changed with the World
Trade Centre terrorist attack. The aftermath of the attack brought needed attention to the vulnerability of modern supply chains (Chapman et al., 2002). This vulnerability can, in many cases, be described as “unwanted effects” in the supply chain caused either by internal or external forces that create disturbances larger than the supply chain is designed to handle. One of the many causes of these disturbances in the supply chain is the problem of cargo theft. No country, no commodity and no shipper are exempt from the acts of cargo theft (EC, 2003). It has been shown that cargo theft is a grave threat to modern trade (EP, 2007). The effects from a cargo theft incident are most often misunderstood and underestimated. Different preventive measures have been implemented to mitigate the problem of cargo theft, but the problem persists.

1.2 Research question
The purpose of this paper is to analyse the supply chain relationship between cargo theft preventive measures and the alteration of cargo theft characteristics. The research question in this paper is:

RQ. Why cargo theft, within transport networks, continues to be a significant problem despite the implementation of numerous countermeasures.

2. Frame of reference
2.1 Supply chain and transport networks
The supply chain is a network of autonomous or semiautonomous business processes that produce physical goods or services for customers (Lin and Shaw, 1998). These processes can be in different companies or in the same company. The different building blocks in a supply chain can, literally, be located throughout the world and connected through the use of a transport network. The transport network is designed to use economy of scale when moving products from consignor to consignee in a supply chain, through nodes and links (Stefansson, 2004). Therefore, several different supply chains can be present at the same time and the same place in the transport network. Transport nodes are terminals, warehouses, harbours and airports, and transport links are a means of connecting the nodes.

Looking at transport from a system perspective, we find that logistics is made up of different levels, infrastructure, resources and material known as the three levels of logistics (Lumsden, 1998). These are linked together to build up the transport system. A logistics system consists of links and nodes, where the nodes are geographically fixed points, such as factories and terminals, while the links are the elements connecting the nodes, i.e. the modes of conveyance. Then, considering the different levels of the system we first find the flow of material. To be able to do this, the material flow uses a flow of resources – meaning, trucks, trains, airplanes and ships. These resources need infrastructure like: roads, harbours, airports and terminals. In order to make, the transport system work, two more flows are needed; namely, the flows of information and capital. Altogether, these five elements can be described as the five needs for logistics fulfilment.

The cargo thief aims to remove goods from the goods flow by attacking the movement of resources and the infrastructure it uses. The potential cargo thief attacks the goods flow when the resources and the infrastructure are in a certain configuration, which can be referred to as a theft opportunity. This paper uses theories from
criminology in order to understand the interaction between potential perpetrators and the theft opportunity in a transport network context.

2.2 Elements of crime
Criminology distinguishes three elements of a crime. They are present in all sorts of crime, ranging from occasional violence crimes to advance and complex economic crime (Sarnecki, 2003). In a cargo theft context, the three elements of crime are characterized by:

(1) motivated perpetrator;
(2) the transported goods (object); and
(3) theft preventive measures – aka. transport security (lack of guardian).

The relationship between the three elements is complex and non-linear. This means that a change in one element may either lead to a crime or prevent a crime from occurring. The change in perpetrator’s motivation is not addressed in this paper, unless the change is directly dependent on different features in transport security. With this said, there is a vast number of different theories that offer different explanations and viewpoints regarding the driving force and motivation behind criminal behaviour. This paper addresses the problem with cargo theft. This means that the different transport security activities are seen as the dominant factor in reducing thefts.

2.3 Transport network theft countermeasures
The management approach to reducing the impact of cargo theft is called transport security. Transport security means the interaction between physical obstructing artefacts (locks, fences, closed circuit television – CCTV, etc.) and the intervention of humans, with the aim of reducing theft, sabotage and other types of illegal activity (EC, 2003; EP, 2007). There are different preventive methods that can be use to reduce the risk of a cargo theft incident, but the primary method is to use physical security countermeasures correctly (Mayhew, 2001). These countermeasures include: fences, locks, seals, guards and other types of security systems (Clarke and Homel, 1997). The objectives for these types of countermeasures are to make the theft both harder and riskier to commit. The next important countermeasure is the control and trust of employees in the company. This method targets the internal theft problem and can be subdivided in two parts: present employees’ supervision (Mayhew, 2001) and new employee reference checks (Muir, 1996). These methods are not sufficient without security plans (EC, 2003), risk analysis and employee education (Mayhew, 2001) to reduce the risk of cargo theft.

The configuration of transport networks leads to the need for security measures in different forms, depending on the exact function and appearance of each nod and link. All different theft preventive methods used can be explained with the basic theory of situational crime prevention. The aim is to reduce factors specific to different types of crimes, locations and situations (EP, 2007). The key issue in situational crime prevention is the recognition that a crime often reflects the risk, effort and the payoff as assessed by the perpetrator (Clarke, 1995). The theory of situational crime prevention is based on the theoretical premise of rational choice (Clarke and Cornish, 1985). The rational choice theory (Cornish and Clarke, 1987) states that an individual makes a decision as to whether or not to commit an offence based on an array of inputs.
These include the effort involved, the potential payoff, the degree of peer support for the action, the risk of apprehension and punishment, and individual needs (Reppetto, 1974). The theory does not state that a perpetrator will commit a crime every time an opportunity occurs. Rather, the potential perpetrator makes a calculated decision about the opportunity to commit a crime (Lab, 2000). In short, a perpetrator acts according to the rational choice theory, seeking to maximize its utility with regards to a particular time and available resources (Bodman and Maultby, 1997).

Some of the criticism against situational crime prevention states that this method leads to property crime receiving more attention than is appropriate. Furthermore, situational crime prevention addresses the symptom and not the cause of the crime. This can lead to an excessive trust in technology (Crawford, 1998). Both of these criticisms are valid for the usage of situational crime prevention to hinder cargo theft. Basically, this is achieved by applying the following four prevention principles (Clarke, 1992; Clarke and Homel, 1997):

1. increase perceived effort;
2. increase perceived risks;
3. reducing anticipated rewards; and
4. inducing guilt or shame.

The different situational crime prevention principles are used to different degrees in the crime prevention measures in the transport network, with the main focus on the first two principles.

2.4 The theory of crime displacement

The theory of crime displacement predicts that crime prevention in one area may have unintentional consequences for other areas or situations. This means that crime prevention may not lead to an absolute reduction in crime. The theory of crime displacement is based on the rational choice theory, with the following three assumptions concerning the potential perpetrator and the target (Lab, 2000):

1. Crime displacement assumes that crime is inelastic (Reppetto, 1976). This assumption indicates that the demand for crimes is unaffected by preventive efforts. This is not true, because all crimes are more or less elastic (Hesseling, 1994). Professional criminals are more inelastic, while opportunistic criminals are more elastic (Reppetto, 1976).

2. The perpetrator has mobility (Reppetto, 1976). The perpetrator has flexibility relative to time, place, method and the type of crime committed. In reality, perpetrators are normally limited in their mobility, adaptability and flexibility, relative to a particular crime, place, time and method (Hesseling, 1994).

3. There exists unlimited numbers of alternative targets (Clarke and Cornish, 1985). The perpetrators have unlimited numbers and types of potential targets to choose from. In reality, the number of targets is limited in one way or another (Hesseling, 1994).

The theory of crime displacement states that rational thinking perpetrators with crime mobility will alter their criminal behaviour in response to crime prevention efforts (Lab, 2000). Crime displacement will only occur when the alternative crime has similar
cost-benefit structure rationalised within the perpetrators’ decision process (Clarke and Cornish, 1985). The key element in all crime is the role that opportunity plays, i.e. if there is no opportunity there is no crime (Felson and Clarke, 1998). The object is to reduce crime opportunities, which will lead to a change in all potential theft situations; therefore, crime displacement is a valid theory (Reppetto, 1976).

Crime displacement can occur in several ways. Reppetto (1976) uses five types of displacement – crime, target, method, place and time. Barr and Pease (1990) add another type of displacement, namely the perpetrator. An often-stated opinion about crime displacement is the theory, in its practical usages, that it can induce a sense of disbelief towards crime prevention initiatives (Town, 2001). This resignation against crime displacement is best described by Barr and Pease (1990):

Experience in mounting crime-prevention initiatives shows that scepticism about their worth is often and frustratingly based on the presumption of total displacement […] Most galling is the frequency with which extreme case pessimists are to be found among police officers whose confidence about the crime reduction effects of patrolling choices has failed to be justified by research.

One problem with the crime displacement theory is that it is accepted because it instinctively appeals to people’s common sense. Town (2001) illuminates this problem:

Criminals are, after all, criminals. Stop them in one location and surely they just find another. Common sense is a valuable commodity, but it has its limitations and changes with time.

With this said, total displacement and partial displacement are different things and the usage of common sense is attracted to the idea of total displacement.

The theory of crime displacement does not explain why perpetrators commit a certain crime or why some crimes are more attractive to them than others. Furthermore, it does not explain the perpetrators’ perceptions and reactions to changes in opportunities (Hesseling, 1994). Crime displacement is one probable explanation as to why the criminal pattern changes in a certain system. A practical and common belief about crime displacement is that: “if perpetrators have the ability, mobility and flexibility to exploit the weakest link in the chain, they will do so” (Ekwall and Lumsden, 2007). It is the perpetrators’ ability to organize a successful theft, and their relationship relative to the actors, within the transport network that are the fundamental variables to categorize perpetrators. According to the theory of crime displacement, the crime preventive measures are of great importance to forcing a change in the perpetrators’ decision process. A simplification of the benefit with a crime can be illustrated with the target that the perpetrators want. A potential target (product) needs to provide a good combination of profit and easiness to sell. The cost side of the perpetrator decision process can be simplified with theft preventive measures implemented by the different stakeholders in the transport network.

2.5 The theory of crime displacement in the transport network

The source of risk for cargo theft in the transport network comes from theft opportunities. These opportunities are highly specific and concentrated in time and place. This is the result of required scheduling and fixed assets of the normal activity in the transport network. The risk for cargo theft can be reduced by initiating resilient countermeasures focusing on reducing theft opportunities. These countermeasures are to induce a change in the characteristics of cargo theft, or, more correctly, change the
outcome of a potential perpetrator's decision process. If a potential perpetrator can change the target, method, place or time, they will do so within their own capability. The key aspect to understanding this effect is the knowledge that the potential perpetrator only responds to perceived preventive measures. Dingle (2005) summarizes the crime displacement in the following way: “Given a choice, criminals will choose the easiest route, and will choose to commit crimes that provide the least likelihood of getting caught.”

A model of the crime displacement effect in cargo theft needs to begin with the supply chain concept. This is the system context for the model, which means that the supply chain is elucidated with the five needs for logistics fulfilment. According to the elements of crime theory, there are three elements involved in order to have a cargo theft; namely, perpetrator, object (the supply chain) and the lacking guardian (insufficient supply chain or transport security). The security effort and the potential perpetrator interact, and every time the potential perpetrator changes characteristics in order to use/make the guardian’s insufficient preventive effect. That interaction is the displacement effect in cargo theft.

The elements of crime theory can be used as a foundation for all crimes against logistics activities and supply chains worldwide. This leads to the fact that on the highest theoretical level, all three assumptions of crime displacement are valid. But in reality, all three elements of crime are limited to time, place, motivation, etc. The extension of this must, therefore be, that the smaller parts of the global flow of goods is examined, and it is less likely for the crime displacement theory to be valid, due to the limitations addressed with the three assumptions of crime displacement as a reliable explanation about changes in cargo theft characteristics. The practical restraint this involves for the everyday business cannot be underestimated. The common-sense idea behind total displacement becomes more-and-more limited as the examined system boundaries are reduced. This means that traces of crime displacement should be most noticeable in highly aggregated statistics, while it should be less evident in local geographical areas.

3. Method
3.1 Study outline
The research method used in this paper is deductive; hence, a hypothesis is developed by logical deduction from existing theories. This paper’s hypothesis on cargo theft has been developed from theories of criminology, for applicable use, to strengthen the scientific field of logistics (Stock, 1997). Credibility is substantiated by verifying the deductive hypothesis with four different methods, so-called methodology triangulation (Mangan et al., 2004). The first step used official statistics from several independent sources in both macro (national, state or bigger geographical areas) and micro (county or smaller geographical areas) levels. With this said, valid statistics are difficult to obtain because they are often incomplete or limited in scope (Nowotny et al., 2002). Furthermore, official criminal statistics are also questionable because they contain both actual crimes and unsubstantiated crimes, but lack unreported actual crimes (Lab, 2000). Therefore, statistics are used in this paper with moderation and only to indicate trends and to prove theoretical assumptions. The second step used two different scientific methods; first, a macro-level, qualitative, open and descriptive expert interview, and as a last verification, a micro-level quantitative-closed survey.
3.2 Criminology research regarding crime displacement
The crime displacement theory has been verified in different studies but the actual effect it has on the crime situation has not been clearly established (Rosenbaum, 1987; Gabor, 1990; Eck, 1992; Clarke and Weisburd, 1994; Barnes, 1995; Green, 1995; Anderson and Pease, 1997; Weisburd et al., 2006). This can depend on the difficulty of verified, empirical data from a controlled area and crime type. This can also depend on the fact that some crimes are locked to a specific place, time or method due to some reasons. An example is the sale of illegal products where the place of sale depends more on customer movement than on crime prevention (Weisburd et al., 2006). This problem is not significant for cargo thefts due to that the crime is not dependent on a customer’s movement, but cargo theft is dependent on the flow of goods together with the movement of resources using infrastructure. Therefore, the displacement effect should be larger in cargo theft than in the sale of the stolen products. Hesseling (1994) illuminates usability of the theory of crime displacement in order to explain changes in crime patterns in the following way:

[…] displacement is a possible, but not inevitable consequence of crime prevention. Further, if displacement does occur, it will be limited in size and scope. This conclusion is supported by other review studies on the topic.

The different types of displacement effects can be difficult to prove with statistics due to the limitation in fact about each individual theft regarding facts as: place, target, time of day, modus operandi, perpetrator, etc. Out of all of these facts, target (products), place and method (modus operandi) are the easiest to establish (both in official crime statistics and in interviews). This means that if there is a displacement effect regarding cargo theft in the transport network, it will be found in trends in these three categories (Cohen and Felson, 1979).

3.3 Interviews
To verify the theory of crime displacement, six interviews were conducted with key personnel in Sweden. They all had long recorded experience of both the logistics business and of theft prevention. The interviews represent different aspects of stakeholders in logistics, both today, in their present positions, and also with their experience from previous employments. They were asked the same two questions and the interview was conducted as a conversation, while all normative discussion was forbidden during the interview. This was done with the purpose to get the interviewees to state their true opinion and experience. For the same reason, all interviewees were guaranteed anonymity so that they did not fear reprimands from their employers. The interviews were all completed with a mutual survey of the notes taken during the interview to ensure that they were representative for the interview (Mishler, 1986). The interviewees have long experience as risk managers, security experts, insurance agents and in different logistics management positions.

3.4 The survey
A survey was conducted whereby the respondents were asked to provide their opinions in relation to seven questions. These questions were formulated after the analysis of the interviews was conducted. Therefore, the questions in the survey closely linked both to the interview analysis but also on the elements of crime and the crime displacement theories within a cargo theft context. All questions were designed
to capture changes in theft pattern. Therefore, all questions were given a limited number of possible answers (six to ten options) and the respondents were instructed to rank the different answers. The eventual change in trend was captured by duplication on all questions, where the first version of all questions referred to a past situation (ten to 15 years ago) and the second version referred to the present situation. The same time grouping as used in the interviews.

The survey was conducted in a geographically limited area in Sweden. This means that the transport network terminal within the same city was chosen. The purpose behind this was to establish the cargo theft trend in a way that the potential perpetrators possessed full mobility (the second crime displacement assumption) and that the different targets had similar cost-benefit-structure rationalised within the perpetrators’ decision process (Clarke and Cornish, 1985). This leads to the only big difference between the terminals, from a perpetrator perspective, was their different security level. The chosen terminals all belonged to big logistics networks and the transported goods were thereby of similar types. This resulted into four terminals \(n = 4\) in the city that were suitable for this survey and they all participated in the study.

4. Empirical findings
The result is presented in four steps. First are the official statistics presented and then the interviews and the survey.

4.1 Official crime statistics, macro-level
The development is indicated in the ECMT (2001, 2002) report: “Crime in road freight transport.” The problems with cargo theft, vehicle theft, theft of goods from vehicles and theft of the entire vehicle loaded with goods have increased. In Europe, the theft of cargo carrying vehicles alone has increased by 21 per cent over a five-year period between 1995 and 1999 (ECMT, 2001, 2002). The problem with thefts of goods during transport is, according to the organisation Transported Asset Protection Association (TAPA, www.tapaemea.com/engl/index.html) Europe, Middle East and Africa, also a growing problem. According to their own Figures (which are a fraction of the transport activities within Europe and only representative for their members who transport more desirable goods than in general), both the location and the mode of procedure are distinguishing factors. Both tables only present the distribution between the different types of place/\textit{modus operandi} (Table I) and categorisation of the stolen goods (Table II). Tables I and II contain data from TAPA members with regards to reported thefts of goods (Winterburn, 2005). The common-sense feeling regarding the validity of the crime displacement theory within the transport network is obvious.

The decreasing share of terminal theft in combination with the increasing numbers of attacks outside of the terminal (parking, hi-jack and stolen truck) clearly indicates that, on a macro-level, there has been a change in general cargo theft pattern. This result shall be compared with the increasing number of failed theft attempts, and it points out that the general security level has increased, mainly on terminals, which forces the potential perpetrators to change criminal behaviour if they are acting according to the theory of rational choice. The change in what types of goods are desirable depends more on the general change in customer demand. This means that the causality, from a crime displacement perspective, with regards to the stolen
goods is very difficult to establish. The development in stolen products in the same statistics is presented in Table II.

Resent statistics from TAPA show, comparing the first ten months of 2006 and 2007, that facility and handling incidents (theft, theft from facility and burglary) dropped from 68.3 per cent (342) to 35.2 per cent (145) and that vehicle-related incidents increased from 31.7 per cent (159) to 64.8 per cent (267) (Solnik, 2007). According to Solnik (2007), this is an indicator that the attack against the transport network has moved out from the terminals and into the roads.

<table>
<thead>
<tr>
<th>Modes of theft per year</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal</td>
<td>36</td>
<td>29</td>
<td>22</td>
<td>17</td>
</tr>
<tr>
<td>Parking</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>Hi-jacks</td>
<td>8</td>
<td>11</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>Lost during transit</td>
<td>20</td>
<td>21</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td>Stolen truck</td>
<td>4</td>
<td>4</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>Failed theft attempt</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Fraud</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Airport</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Secure parking</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Illegal</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Share of product types over four years</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers</td>
<td>34</td>
<td>38</td>
<td>56</td>
<td>47</td>
</tr>
<tr>
<td>Mobile phones</td>
<td>10</td>
<td>14</td>
<td>27</td>
<td>19</td>
</tr>
<tr>
<td>IT components</td>
<td>22</td>
<td>49</td>
<td>34</td>
<td>29</td>
</tr>
<tr>
<td>IT peripherals</td>
<td>12</td>
<td>34</td>
<td>50</td>
<td>27</td>
</tr>
<tr>
<td>IT supplies</td>
<td>2</td>
<td>3</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Various IT (mixed)</td>
<td>9</td>
<td>11</td>
<td>35</td>
<td>42</td>
</tr>
<tr>
<td>Consumer electronics (non-IT)</td>
<td>11</td>
<td>33</td>
<td>57</td>
<td>57</td>
</tr>
<tr>
<td>Non-electronic</td>
<td>12</td>
<td>25</td>
<td>49</td>
<td>63</td>
</tr>
<tr>
<td>Cash/bullion</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Unspecified</td>
<td>3</td>
<td>25</td>
<td>16</td>
<td>48</td>
</tr>
</tbody>
</table>


4.2 Official crime statistics, limited geographical area

Within a geographically limited area in Sweden, the local police have given the criminal attacks against road transports extra attention. They have observed and followed-up on all reported crimes towards trucks. The within one police district were there 95 attacks in 2006 and 73 in 2007 (Randåker, 2007). The same years were the reported attacks against transports 512 (2006) and 476 (2007) in the southwest of Sweden. The attacks occurred mainly along the major roads (Nilsson, 2008).

A first glance indicates a change in criminal pattern. During this period, the problem of attacks against trucks received more attention than before.
According to Randåker (2007) and Nilsson (2008), this may have led to a change in criminal pattern, in which the potential perpetrators attack shops instead.

### 4.3 Transport network expert’s interviews, macro-level

**Q1.** Describe cargo theft and preventive measures in the logistics business ten to 15 years back in time.

The problem with cargo theft in the transport network was (proportionately) common in terminals. The perpetrators did not see themselves as thieves in the word’s proper meaning. They saw the actual theft as a wage benefit. The place for the theft was often in a terminal where the thieves worked. One of the interviewees describes the problem as: “an item became a box, became a pallet.” This development can be described as cargo theft evolving into a professional activity from being a pilferer by nature. The theft characteristics transformed from a self-persuaded wage benefit from becoming more of a business enterprise with the object of selling the stolen goods.

The direct countermeasures taken by the logistics business were to bring terminal security in focus. The business discovered that they had no, or very little, control over which people were on the terminal or what they were doing there. The preventive action taken was to limit access to terminals and increase supervision of the staff. It worked, and the small opportunistic thefts were reduced. When terminals become riskier for the potential perpetrator, the theft from trucks and containers between terminals increase substantially. In the early 1990s, the trend of stealing fully loaded trucks began. The target, method, place and time of thefts in terminal change because of the improved security there, and other parts or links in the transport network became the weaker spots from a security point-of-view:

**Q2.** Describe cargo theft and preventive measures in the logistics business today.

The internal opportunistic theft, in the form of pilfering, has, nowadays, almost vanished. This development depends most likely on better control over both staff and cargo. Both the volume and the value of stolen goods have increased greatly from the 1980s to today. The perpetrator knows the location of the goods in a way that in many cases can be explained only by their having access to inside information, one way or another. The revolution in information technology has made it possible for criminals to get information about cargo in more ways than before. The information of the load or goods has increased in importance for both the company and for the perpetrators. This leads to the IT security being an important part of transport security.

The security in terminals has improved but there still exist a few terminals without any security equipment at all. The countermeasures implemented by companies have improved control over both employees and the goods. The consignor of the cargo demands better security, and the suppliers of hi-tech equipment are the driving force. The security in terminals has become so good that it has forced the perpetrators out on the roads instead. During the last decade, so-called hi-jacking of trucks, which is a form of armed robbery and theft of the entire vehicle, has become more-and-more common. One interviewee claimed that: “the perpetrators have in many cases better knowledge about technology, organization and transport network activities than the involved companies”. This gives the perpetrators the opportunity to really attack at the weakest point in the transport network. All interviewees stated that: “The perpetrators have
been forced to specialize, to be able to continue their profession.” An unfortunate consequence of the specialization is that they have also developed their sales network to be able to handle larger volumes of stolen goods.

Since the business, at a larger scale and as a general trend, began to prevent cargo theft, the cost for prevention has increased and the number of thefts declined. Most of the declines in the number of thefts were opportunistic thefts committed by employees. According to the three assumptions about crime displacement, the opportunistic theft is not affected by the first of them. The decline in opportunistic thefts combined with the first assumption (opportunistic thieves are not affected by displacement) about crime displacement, indicates that the displacement effect in cargo theft has become more obvious. This gives the theory of crime displacement in the transport network more credibility. During the same time, the value of the stolen goods has increased, which indicates that the volume also has increased. This trend demonstrates that the perpetrators steal the goods in order to convert it to money. The perpetrators are becoming more professional in a general statement about cargo thieves.

4.4 The survey, limited geographical area
The result from the geographically limited survey \((n = 4)\) is presented in Table III. Only the top three to four of all given answers are presented. The answers from each participant in each category were ranked (the top answer received the highest value \((6-10)\) while the value \(1\) is lowest). The respondents were given the option not to rank (ranking value zero) an answer if it was not suitable. The result is presented with

<table>
<thead>
<tr>
<th>From 10 to 15 years ago ((Q1))</th>
<th>Today ((Q2))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crime type occurrence (eight options)</td>
<td>7,8: Theft from loaded vehicles</td>
</tr>
<tr>
<td></td>
<td>7,0: Theft from terminals</td>
</tr>
<tr>
<td></td>
<td>3,8: Theft of loaded vehicles</td>
</tr>
<tr>
<td></td>
<td>3,3: Theft of loaded vehicles</td>
</tr>
<tr>
<td>Crime type serious (eight options)</td>
<td>6,8: Theft from terminals</td>
</tr>
<tr>
<td></td>
<td>5,5: Theft from loaded vehicles</td>
</tr>
<tr>
<td></td>
<td>5,0: Theft of loaded vehicles</td>
</tr>
<tr>
<td></td>
<td>3,0: Theft attempt (vehicles)</td>
</tr>
<tr>
<td>Cargo type with regard to theft risk (ten options)</td>
<td>7,0: Computers</td>
</tr>
<tr>
<td></td>
<td>5,8: Mobile phones</td>
</tr>
<tr>
<td></td>
<td>4,8: Unspecified</td>
</tr>
<tr>
<td></td>
<td>4,8: White goods</td>
</tr>
<tr>
<td>Cargo type with regard to volume/theft (ten options)</td>
<td>7,0: Computers</td>
</tr>
<tr>
<td></td>
<td>4,8: Unspecified</td>
</tr>
<tr>
<td></td>
<td>3,8: Mobile phones</td>
</tr>
<tr>
<td></td>
<td>2,3: White goods</td>
</tr>
<tr>
<td>Terminal security measure (six options)</td>
<td>4,8: Locks on doors/windows</td>
</tr>
<tr>
<td></td>
<td>3,3: Fences</td>
</tr>
<tr>
<td></td>
<td>3,0: Security procedures</td>
</tr>
<tr>
<td></td>
<td>3,0: CCTV</td>
</tr>
<tr>
<td>Vehicle security measure (six options)</td>
<td>3,0: Security procedures</td>
</tr>
<tr>
<td></td>
<td>2,5: Mechanical locking device</td>
</tr>
<tr>
<td></td>
<td>1,0: Alarms and sirens</td>
</tr>
</tbody>
</table>

Table III. Mean value result from the limited geographical area survey
mean value (total ranking value divided with the number of terminals \(n = 4\)) in Table III.

The results clearly indicate that the changes are insignificant, but, nevertheless, there are changes in the pattern. The different security measures are similar, now and then: the big difference is the increased belief in security procedures and CCTV in terminal security but also the increased emphasis of vehicle security efforts. This shall be compared with the change in seriousness about crime type; there robbery of goods from terminal has become a real threat.

The general analysis from the survey is that a crime displacement effect is difficult to verify. This can depend on the limitation that the survey designs itself imposed or the fact that the displacement effect is not visible in clearly limited areas. The survey misses if the potential perpetrators change their criminal behaviour outside the four terminal areas. This means that the full criminal mobility of the perpetrators where not within the researched zone.

5. Analysis

5.1 Macro- and micro-level analysis
Interpreting at Table I indicates that thefts in terminals have decreased during these four years while the thefts in parking spaces, as well as hi-jacks and stolen trucks, have increased. This indicates that the trend is, in relative terms, that cargo thefts have changed modus operandi to attack transports more instead of terminals than before. This trend indicates that the perpetrators have more crime mobility than before. According to Saunders (2008), is it possible that “some perpetrators respond to sophisticated transport security measures by increasing their use of unsophisticated and brutal violence against drivers and terminal personnel”. Similar development is expressed by EP (2007): “The criminal organisations seem to react to the increased security with more aggressive methods.” These statements have support as both the official crime statistics macro-level (Section 4.1) and the survey indicates that robbery and hi-jacking of trucks are increasing. Saunders (2008) and EP (2007) refer to a partial displacement regarding method.

The perpetrators can, from a system point-of-view, change place and method, while Table II indicates that that actual target (type of goods) has a lesser changing trend. This can depend on the fact that the type of goods that the thieves are interested in are decided by their customers instead of theft opportunities within the transport network. The similarity with the discussion on place of sale for illegal products is striking (Weisburd et al., 2006). With this said, the perpetrators have changed their modus operandi in order to steal the same type of products from the transport network. The interview indicates that the security efforts from the transport network addresses first the terminals, and that they also record a change in theft pattern, primarily place and modus operandi but not type of product. The crime displacement effect may be one likely explanation for this development. The interviews also indicate that the cargo thieves are becoming more and more professional. The same trend is visible in the macro-statistic (a hi-jack is normally considered more difficult to accomplish than a theft). This means that the first assumption for crime displacement (crime is inelastic) is more valid which leads to that a crime displacement is more likely to occur. The two geographically limited studies clearly indicate the difficulty on a local level (where each potential perpetrator actually can have full crime mobility (second crime displacement assumption)) but limited
numbers of alternative targets (third crime displacement assumption) to verify crime displacement as explaining changes in criminal pattern. This leads to the conclusion that all three crime displacement assumption is easier to fulfil on a macro-level then on a micro-level, which is one interpretation of why crime displacement is visible at macro-level but not at micro-level.

5.2 Crime displacement in cargo theft
The common-sense belief in crime displacement effects within the transport network is based on macro-level statistics, which clearly indicate changes in theft pattern, but also in preventive measures taken by the business. The prevalence of the belief that perpetrators always attack the system in the weakest point is an attractive common-sense conclusion, but as indicated by both the research presented in this paper, as well as in several other papers, the causal relation between the perpetrators’ decision process and the crime preventing measures are difficult to verify. This fulfils Hesseling’s (1994) conclusion about crime displacement, namely: “crime displacement is a possible, but not inevitable consequence of crime prevention. Further, if displacement does occur, it will be limited in size and scope.”

6. Conclusions
Where there is a logistics flow there is always a risk for having the goods stolen. If this risk source to disturbance in the supply chain is not taken seriously it will increase, in the long-term, the cost for the supply chain. The theft risk arises from different theft opportunities that will always be present in a transport network. These opportunities can be reduced by the usage of situation crime prevention methods. Correct countermeasures alter the potential perpetrators’ decision process in a way that simply can be described as the perpetrator seeking the weakest point within their capability to continue stealing.

The theory of crime displacement in the transport network states that within the potential perpetrators’ capability, they will change their criminal pattern in response to countermeasures implemented by the business. Of the six displacement types, the change in place and modus operandi are easiest to both measure and establish. There has been a lesser change in the type of products that are stolen from the transport network. This correlates with the fact that it is not the thieves but the buyers of stolen products that govern the choice of target, while it is the potential perpetrators that decide where and how to acquire the products. The crime displacement effect may be one likely explanation for this development.

The common-sense feeling about the crime displacement theory that exists in the logistics business needs to be modified. Owing to the total displacement and partial displacement, these are different things and the usage of common sense is attracted to the idea of total crime displacement. For the practical theft prevention in the transport network, the total displacement idea seems useful, but in reality, it is more useful for the locals to understand and know about modus operandi, perpetrators’ motivations, etc. in order to introduce the right theft prevention features. This paper has demonstrated that the causality in crime displacement is difficult to establish. The same conclusion has been presented in several other papers regarding the validity of the crime displacement theory.
References


Further reading


Corresponding author
Daniel Ekwall can be contacted at: Daniel.Ekwall@hb.se

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints
ABSTRACT

Purpose of this paper

To provide explanations and understanding of how logistics business actors, by using cargo liability regulations in order to minimize negative business impact, both contribute to and use business complexity to handle supply chain risk.

Design/methodology/approach

The research is based on a system-theoretical approach, which emphasizes a holistic view instead of the characteristics of the different parts. The research method used in this paper is deductive. The analysis is based on complexity theory with regard to logistics business actors’ cargo liability toward the goods owner in case of cargo theft incidents.

Findings

The handling strategy used by the different logistics actors is similar to the idea of the Old Maid game. The Old Maid game strategy is a defensive strategy and aims only to avoid losses. The effectiveness of this strategy depends on the number of participants. The basic idea is to hide in numbers. The Old Maid game strategy becomes more useful if either the number of participants or business complexity increases, or both.

Research limitations/implications (if applicable)

This research is mainly conceptual, but shall be seen as a theoretical contribution, explaining both the everyday business behaviour and the failing of supply chain collaboration.

Practical implications (if applicable)

The research aims to provide a better understanding for why logistics actors emphasize liability borders as a risk reducing phenomenon.

What is original/value of paper

This paper introduces the Old Maid game strategy as a risk reducing approach, and thereby, also, a cost reducing defensive strategy used by transport network actors.

Keywords: Risk management, Supply chain risk, Insurance claims, Cargo liability, Logistics business strategy
1. INTRODUCTION

The international trading system depends on effective transportation of goods. During a transport from consignor to consignee, various things can occur that affect the quality of the transport. There can be a delay or cargo damage incidents can happen. But, also, criminal activity can take place that affects or even hinders the transport from reaching the consignee. The theft of cargo value for the EU-area is estimated to be €8.2 billion each year, which allocated on all transports, gives an average value of €6.72 per trip (EP, 2007). Cargo theft generally has had a low priority status in most countries and is often perceived largely as the cost of doing business (EC, 2003).

1.1. Problem description

To attain an effective and smooth transport, several companies are normally involved as each company provides their core competence and core activities to the flow of products. When something happens with the transport, regardless of what, one of the companies involved is considered responsible for the cargo. That company is the one who should investigate the incident and take proper action according to the agreements with the cargo owner. A simplistic view on this, as proclaimed in the logistics literature on supply chain collaboration/cooperation, is that the responsible organisation solves the problem, or, at least acts according to the agreement with the goods owner.

However, while logistics theories often are based on simplifications, such as objectivity, rationality and determinism, real-life logistics practice is characterized by last-minute changes and rearrangements due to different people’s interpretations; accidents; changes in customer demand; machine and computer breakdowns; mistakes and thefts. The apparent difference in theory and practice is paradoxical in its nature and certainly of misleading character in many contexts and situations. Reality changes unpredictably, sometimes in outrageous ways based on both the cooperative and opportunistic behaviour of its actors.

The paradox of cooperation/competition is one to be found in logistics. It is based on striving for the “ideal” cooperative situation of a supply chain as a single unity with unifying goals, and in that striving, subjectivism, power and avoidance of conflict are hidden. While a vision of an ideal situation and overall harmony is laudable - and hopefully something that one day can be realized; in today’s world, one must question how realistic such beliefs are. As Mears-Young and Jackson (1997, p.610) state, “the aims of logistics rest upon the assumption that all members of the organization can be brought into agreement.” The examples supporting this statement can easily be found; for example, Lambert, Cooper and Pagh (1998, p.9) state that the lack of inter-company consistency in different company structures or differences in naming activities and processes is: “cause of significant friction and inefficiencies in supply chains.” Furthermore, Yu, Yan and Cheng (2001) state that supply chain management: “emphasizes the overall and long-time benefit of all parties on the chain through cooperation and information sharing.” Finally, Gentry (1996, p.36) refers to the chain viewed as a whole, “a single entity rather than fragmented groups.”

The question of who really should have unified views and common goals is never asked. Furthermore, who should cooperate is never addressed. In addition, how should the unifying goal be set and achieved? In the literature available, it is said that the firms leave the interpretation space wide open for subjective interpretation. In this regard, Johannessen (2003, p.11) declares: “The everyday conflicts and unpredictability of human relating is not
examined and explored, leaving the recommendations seemingly easy and straightforward to adopt and implement in any organization.”

1.2. Research purpose

In this paper we aim to address this paradox of cooperation/competition when handling risk, especially in the relationships among actors involved in the transportation of goods. Hence, the purpose is to provide explanations and understanding of how logistics business actors, by using cargo responsibility regulations, cargo liability, in order to minimize negative business impact, both contribute to and use business complexity to deal with supply chain risk.

1.3. Research approach

The idea underlying the research in this paper derives from data obtained in previous research (Ekwall, 2007). The comment was: “we have installed surveillance equipment to verify if we were responsible, if the customers claim it.” The comment contains two key elements: responsibility and claims as central aspects that must be handled one way or another in business relationships. A system theoretical approach has been used in order to illuminate these aspects in the context of transportation. This, since the emphasis for a holistic view instead of the characteristics of the constituent parts is needed to understand the complexity among the actors. This means that the macro system is the entire transport network that consists of all involved organisations to fulfil transport demand worldwide (while this includes several modes of transportation the main focus of the paper is on land transportation). The transformation process in this system is the transport chain from consignor to consignee. The constraints that limit the transformation process are, in general, aspects such as: cost, time, quality, security, information, etc. In each of the involved organisations, the same system description will be valid. For example, the goal for each organisation will be to make profit by fulfilment of the customers’ demand. The profit is the difference between price and cost/risk.

The cargo liability constraint is essential in this paper to understanding the relationship between cargo owner and freight forwarding actors. If something happens with the cargo during transportation, then the contract between owner and handlers becomes decisive about who will take care of what and at what cost. In such situations, the question as to who is responsible when an incident occurs is of crucial importance to all involved actors.

1.4. Paper structure

While this paper is mainly conceptual and shall be seen as a primarily theoretical contribution, i.e. deductive in its nature, it provides implications for the everyday business behaviour as it elaborates on the context of transportation networks. This paper is structured according to a clear deductive approach, where the frame of reference leads to the conceptual theoretical construction. The deductive approach helps to substantiate the objectivity of this research (Popper, 1959). The conceptual theory is verified in two steps: first, with the use of complexity theory within the system context, and secondly, with two illustrative cases based on one of the authors experience in industry. The cases portray different perspectives on the practical usage of risk transferring between actors in the transport chain with focus on the borders of liability between the actors.
2. FRAME OF REFERENCE

2.1. Transport networks

The different building blocks in a supply chain can, literally, be located throughout the world and connected through the use of transport networks. These transport networks are designed to use economy of scale when moving products from consignor to consignee in a supply chain, through nodes and links (Stefansson, 2004). Transport nodes are terminals, warehouses, harbours and airports, and transport links are a means of connecting the nodes. The transport network affects cost throughput time and if used wisely, it can increase the value of the product (Lambert et al., 1993). According to Zsidisin and Ellram (2003) a delivery failure or incident can cause detrimental effect throughout the entire supply chain and ultimately reach the end-user. This is, therefore, a supply chain disruption of concern for all involved actors.

2.2. Business complexity

The principles of complexity theory suggest that physical, social, and mental worlds are nonlinear and complex. The perception of supply networks and logistics as being complex is emphasized by several authors (Christopher 1998; Cox 1999; Lambert, Cooper & Pagh 1998; Tan 2001). Milgate (2001, p.107) observes that: “complexity should be viewed as a deterministic component more related to the numerosness and variety in the system.” i.e. logistics systems could and should be heavily reduced and simplified in order to be dealt with. There are several others proclaiming the same simplifying approach to deal with logistics complexity (Childerhouse and Towill (2003), Narasimhan and Jayaram (1998), Towill (1999), Towill, Childerhouse and Disney (2000)). However, Choi, Dooley and Rungtusanatham (2001), Johannessen and Solem, (2002) and Nilsson (2005) question these simplified and reductionist approaches. Instead: “logistics processes, where human beings are involved, are not simply a sequence of mechanical devices which can be assumed to work along positivistic beliefs, but instead a complex network of living, innovative, creative, and evolving creatures which react and adapt dynamically to their perceived environment, and try to proactively create what they themselves, or collectively with others, find to be beneficial for their own interests” (Nilsson 2005, p.35). With such a perspective on logistics, the reality of transportation issues can be examined and the empirically identifiable actions, such as minimizing personal losses, wishes for blurry borders, keeping oneself out of trouble, etc. can be better understood.

Insights from complexity theory guides the search for a few guiding principles that together describe the behaviour of the system (Gault et al., 1996). To think in terms of complexity means to appreciate the idea that every change affects, in non-linear ways, other involved parts of the system. The complexity theory gives us a system understanding that is based on subjectivity and paradoxes instead of objectivity and rationality in interaction between actors (Macbeth, 2002).

In close relation to complexity is uncertainty, as underlying principles of determinism and predictability are wishful for business. Certainty in business means that every factor is fully deterministic and the outcome will be fulfilled in a precise manor. However, uncertainty is simply a key characteristic of any economic activity (von Oetinger, 2004) and with the uncertainty comes risks. A major consequence that uncertainty brings in business is that each
actor, as rationally as it can out of its subjective perspective, tries to control and reduce the uncertainties it is exposed to.

While knowing and predicting what customers want often involves a great amount of uncertainties, it is only one of many questions to be answered. Each manager also needs to answer the question as to when, how and why the customer wants a certain product, and how it is possible to get it to the customer; i.e., logistics uncertainties. According to Nilsson (2006) logistics uncertainty can be grouped into four different dimensions, namely: 1) Customers demand and expectations, 2) Internal processes, 3) Human factors, and 4) General trends. All four dimensions of logistics uncertainty will, to varying degrees, be put throughout the transport network. This indicates that the complexity within the transport network is increasing due to uncertainty in different dimensions. According to Nilsson (2006) the message in logistics literature is that the treatment for uncertainty is to reduce it as much as possible. This is also, as mentioned above, the valid view on complexity. The different actors within the transport network handle its complexity in similar ways: all actors are, to varying degrees, involved in activities that aim to reduce, or at least limit, the complexity—their own, and that of the transport network. The more complexity in the transportation network, the more complexity is transformed throughout it. This development increases the need for handling strategies that reduce the effects from complexity. This paper aims to illustrate one strategy that is used to reduce the effects from business complexity that emanate from the complexity itself. The iterative results of these processes are paradoxical situations where the interests of different groups of people (i.e. divisions, departments, functions or firms) are continually creating opportunities; at the same time, these processes restrain the developments of other processes.

### 2.3. Supply chain risks

With uncertainty comes risk, not at least in logistics. Today, risk is a factor of consideration in all business functions and processes (Cavinato, 2004). This refers to the concept that every function or process has a certain probability of not performing as planned; i.e. disrupted in some way, and that there is a certain consequence attached to that probability.

The search for minimizing personal business risk has always been a part of doing business (Waters, 2007). However, minimizing business risk often leads to minimizing the profit from the business as well. Consequently, a pursuit for the optimum balance between potential profit and risks, which is normally called risk management, is searched for. Risk management is, according to Hardy (1999), not a separate activity from management, it simply is management. This paper uses the same approach towards risk management and management, but, in order to avoid confusion uses the term risk management.

According to Christopher and Peck (2004 - a), risk sources for a supply chain can be divided into three categories; namely: internal, external and environmental. Internal risks can be further subdivided into process and control risks. Internal supply chain risks come from a lack of visibility and ownership, self-imposed chaos and the misapplication of Just-in-Time logistics, as well as inaccurate forecasting (Chapman et al., 2002). External risks can be subdivided into demand and supply risks. Demand risks are associated with outbound logistics and uncertainties in product demand (Svensson, 2002). Supply risks are instead associated with uncertainties in inbound logistics (Zsidisin et al., 2000). The external risks can also be described as risks emerging from the interaction between the supply chain and its environment (Chapman et al., 2002). Sources of environmental risks are: politics, nature and social uncertainties (Juttner, 2005). Studies of supply chain risks seldom address these
different causes to risks (Christopher et al, 2004 – a; Christopher et al, 2004 – b; Juttner, 2005; Sheffi, 2001). They simply mention supply chain risk sources without talking about causes like theft, smuggling, sabotage and other criminal activities other than terrorism. Not all supply chain disruptions are caused by criminal activities, but many are. With this said, the discussion of risks in the supply chain is a good way to describe negative effects in the chain. Consequently, many actors focus on reducing consequences for their own business by transferring the risk to someone else that is able or willing to handle it (Waters, 2007).

2.3.1. Supply Chain Risk Management

Basically, there are four different strategies or methods in order to handle the risks (Wang et al., 2000); 1) Avoidance: Discontinue the practice that creates the risk, 2) Mitigation: Implement strategies to reduce the impact, 3) Transfer: Transferring the risks with contracts or insurance policies, and 4) Acceptance: Live with the risk.

The primary method is risk avoidance, but this strategy also means avoidance of income from the same risk source. Therefore, risk avoidance is an inadequate strategy in order to obtain optimum balance between profit and cost/risk. The same discussion is valid for risk acceptance but with inverted intention. This leads to only two basic strategies being valid for managing the balance between profit and cost/risk, namely, mitigation and transfer. In practical use there is no clear distinction between the two strategies, as mitigation of a risk can be seen as transfer and vice versa. The general idea in this paper is that actors seek to transfer cost/risk but still keep the profit from a certain transaction. This is all done in order to obtain the highest possible income from a business deal, but avoid as large a share as possible from both costs and risks attached to the same business deal. This general strategy is illustrated in this paper within a transport network context, but is valid for other business behaviour as well.

2.3.2. Risk transfer within transport networks

According to Wang and Rouch (2000) risk transfer is a common strategy to achieve risk control. The basic idea is: by transferring the risk to someone else, it reduces personal risk substantially, by using different types of contracts. This strategy is surprisingly not mentioned in several papers which addresses the issue of supply chain risks (Christopher et al, 2004 – a; Peck 2005; Juttner, 2005; Sheffi, 2001), while it is common knowledge that the risk transferring strategy using insurance and contracts are closely embedded in all business relationships. The logistics business is not exception. In freight industry, liability insurance is one of the best examples of the risk transfer strategy. The key element in liability insurance is normally the contract between the involved parties. In order to simplify business relationships, several conventions (e.g. CIM, CMR) have been developed. If nothing else is contractually decided, these conventions are contractual agreements. There also exist a number of standardised contracts regarding risk regulation (Incoterms and NSAB) (Stöth, 2004). Mutual for all these is that they govern compensations and responsibilities between goods owners (both seller and buyer) and freight forwarder actors. These conventions and standardised contracts work according to the general insurance principle.

The insurance principle prescribes that the insurance company takes over the economical impact if something covered within the insurance contract happens. This means that the risk for this to happen needs to be rather easy to identify, classify and determine. All in order for the insurance company to estimate the cost related to the risk, and thereby, determine the insurance premium. This premium is also accompanied by an insurance excess. This gives the
potential insurance buyer three components to consider, namely: the terms, premium and the excess of the specific insurance. The incentive for each individual insurance buyer is thereby the central issue, and in extension, also the potential reduction of a potential loss (Keller 2003).

According to Stöth (2004) the key element in all types of liability contracts is the usage of clear and distinct borders of responsibility. This makes it easier to establish who is responsible if something happens unexpectedly. The contract shall also account for what this responsibility means, something the CMR convention covers. However, this means that if nothing else is agreed upon in a contract between the involved parties, the CMR is the rule for the risk transfer strategy. Despite that, the majority of a major loss will lead to some kind of negotiation between the insurer and the client (Garrett et. al., 2003). These post-contractual negotiations can be not only costly but also lead to an abuse situation within the insurance policy (Garrett et. al., 2003).

The key element of liability insurance is that goods owners take a major of the risk if nothing else is decided (Stöth, 2004). The different actors within a transport chain never take over ownership of the transported goods, only the liability of it. This means that the goods owner, in order to achieve full risk transfer, needs to have property insurance while the logistics actors need liability insurance. The differences between property and liability insurance can, of course, also be stipulated in contracts between the parties. According to Doherty and Schlesinger (2002) the marketplace for liability insurance is expanding. The insurance companies offer more and more different types of professional liability insurances. This leads to all involved actors having more opinions and possibilities to optimize their risk taking.

S. Hun Seog (2006) defines the general idea behind the usage of insurance in business the following way: “The optimal coverage is positive if the strategic effect is greater than the cost of insurance. The main strategic effect of insurance comes from the fact that firms purchase insurance before they produce outputs. Insurance makes firms more aggressive due to the limited risk costs of firms.”

In order to hinder an uncontrolled outcome from a specific insurance policy, it is normal to use a limitation of the potential maximum payout for a single event. This leads to the fact that a specific insurance cover can be divided into several different insurance policies, where they all have their own premium and excess based on the potential risk cost for each specific insurance policy. A major advantage with this strategy is that the first insurance policy is designed in order to handle the most frequent occurring payouts, while the other policies are designed more and more to limit the single maximum payout for a specific event (Garrett et. al., 2003).

The principle with different insurance policies can also be used to handle/transfer different types of risks. Each insurance policy shall clearly state different insurances terms. According to Spekman and Davis (2004) companies can, by interruption/denial of service, transfer the risk of a potential financial loss due to a security breach or other types of incidents that normally are covered with special insurance policies. According to Garrett and Marshall (2003) a common risk strategy for an actor is to own only a minor part of the equipment they use. This depends mostly on the fact that the risk for ownership is transferred.
The CMR convention

In order to set up clear rules and regulate responsibilities in international trade, the UN published the first edition of the CMR (Convention on the Contract for the International Carriage of Goods by Road) convention in 1956. The purpose was expressed as:

“Having recognized the desirability of standardizing the conditions governing the contract for the international carriage of goods by road, particularly with respect to the documents used for such carriage and to the carrier’s liability” (UN 1956)

The desire to regulate the transport industry by developing a standardized set of liability regulations was obvious. The development of the CMR convention is still an ongoing process, but the main frame was set in the first edition from 1956. The international community has established regulations for Sea and Air freight as well. The main focus in these three different regulating documents is similar: to standardize the liability between carrier, freight forwarder and goods owner in the international trade.

The CMR regulation contains 51 articles that are divided into eight chapters. For this paper, the articles 17, 23 and 29 are of particular interest. These are in the fourth chapter named “Liability of the carrier” (UN, 1956). The articles describe the three main carrier and freight forwarder liability categorizations, namely: no-liability, limited liability and full liability. These articles govern the responsibility of the carrier regardless as to whether the ground for the liability dispute is damage or theft of the goods. A general view of the content in these three articles can be expressed in this way. From no liability at all, via limited liability to unlimited liability (Spiegel, 2007). If such a thing as a normal state can be expressed in terms of carrier liability it would be limited liability. All discussion of the carrier liability, can, in this paper, only be theoretical. In practice, the discussion is living and often handled through courts in different countries. With this said, the general view presented in this paper is the same as the general content in the living discussion.

The carrier can invoke the no liability to a claim or the “Force Majeure” to the claim. According to Spiegel (2007) the precedent comes from a court verdict from 1998, the “Oegema/Brada.” This verdict shows that: carrier must demonstrate that he has taken all measures to prevent loss, which a diligent carrier – including the persons whom the carrier engages in the performance of the contract – would take in the given circumstances (ibid.). The main focus here is that the carrier must have taken all measures in order to avoid the loss. In reality, the consequence of this principle is that Force Majeure is hard to plead for the carrier, even if the loss was caused by an armed robbery (ibid.).

The opposite of Force Majeure, or no liability, is Gross Negligence or full liability. This means plainly that the carrier compensates the full value of the lost goods to the goods owner. According to Spiegel, the precedence is a court verdict from 2001: the “Cigna/Overbeek + Van der Graaf/Philip Morris.” The main issue is: Carrier acted recklessly, and with the knowledge (subjective!) that the chances that damages would occur were considerably higher than that they would not, but acted accordingly anyway (Spiegel, 2007). The key point is that the carrier had knowledge about the increase in risk for losses from a certain action made.

In order to solve an accusation of Gross Negligence, the goods owner or the carrier company (the one who is first) takes legal proceedings on one of the countries that the transport passes through during the freight. The prosecutor chooses the country in which they think that they have the biggest chance of winning the courts approval. According to Spiegel, there is a big difference between courts in the Netherlands and Germany regarding the possibility of having
a liability issue considered a *Gross Negligence* from the carriers’ side, where Germany is more likely to judge in benefit for the goods owner.

2.3.3. Enhanced liability in insurance

The term enhanced liability refers to a contract obligation between goods owner and logistics service provider (LSP), where the LSP have accepted extended liability for future claims payments beyond normal standards of transport law, conventions (CIM, CMR) or national standard terms and conditions (Incoterm, NSAB) for freight forwarders. This means that the goods owner has transferred parts of his risk over to the LSP. The same principle is valid for the contractual relationship between the LSP and a carrier company. In general, enhanced liability is a practical strategy to transfer risks from one part to another part in a contract. The receiver of the enhanced liability can sign a special insurance policy that only covers the enhancement of the liability. These enhanced liability insurance policies are constructed in the same way as all insurance. They can be limited and specified with different terms, premiums and excesses.

3. CONTEXTUAL DESCRIPTION

3.1. Generalisation of the transport network actors’ pros and cons

The complexity within the transport network makes it difficult to generalise. As is the case of unplanned events, the number and variety of actors involved increases (e.g. insurance companies, authorities, police etc.). However, for the purpose of this paper, a generalisation of the actor’s pros and cons will, in the transport network, be categorized into three components, namely: earnings, costs and risks. Pricing and marketing strategies can affect the earnings, i.e. the pros, for the actors. The pros are not addressed in this paper, and therefore, are effects from cargo theft incidents not described as having an income reductive effect. In reality, a cargo theft incident will likely cause some kind of effect, at least some kind of goodwill loss. The actor’s cons are separated into two categories: costs and risks. This separation is mainly a theoretical construction where the risks could also be seen as latent costs or potential costs. The cost component is reduced with the economy of scale in operations and other cost reductive focused initiatives. The minimization of risks can be seen as a cost minimization strategy. The logistics actors try to minimize their own part of the total transport chain risk, and thereby minimize the potential costs from failures. The actual handling of risks within the transport chain is done with contracts, borders of responsibility and the use of insurance. The main idea behind this is to handle the economical impact of an incident by sharing or diluting the costs on all participating logistics actors. The generalisation of the actors within the transport networks pros and cons are illustrated in figure 3.1.
3.2. Transport network actors

The actors involved in the transport network are shortly described below in table 3.1. Mutual to them all is that they try to maximize their profit; in other words, the difference between earnings and cost/risk in their business (Cavinato, 2004; Waters, 2007). This process is what Hardy (1999) describes as intertwining of risk management and management.

**Table 3.1 Transport network actors and their wants and needs**

<table>
<thead>
<tr>
<th>Actor</th>
<th>Wants and needs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consignor</strong></td>
<td>Wants the goods to be delivered to the consignee on time (Giunipero, 1990), undamaged (Giunipero et al., 2004) and at a low cost (Tan, 2002).</td>
</tr>
<tr>
<td><strong>Consignee</strong></td>
<td>Wants the goods on time (Giunipero, 1990) and undamaged (Giunipero et al., 2004).</td>
</tr>
<tr>
<td><strong>Logistics Service Provider</strong></td>
<td>Wants to fulfill the demanded transport between consignor and consignee (Stefansson, 2004), but in order to have an adjustable capacity (Garrett, 2003; Tang, 2006), and thereby have the opportunity to let the personal cost follow the income (Tang, 2006); they don’t own any trucks, just terminals.</td>
</tr>
<tr>
<td><strong>Hauler</strong></td>
<td>Provides the trucks to the LSP, but in order to have an adjustable capacity (Tang, 2006) they just act as an information broker to their attached independent drivers, who own their trucks (Garrett, 2003).</td>
</tr>
<tr>
<td><strong>Insurance company</strong></td>
<td>Based on different cost/benefit calculations they provide insurance services (Doherty et al., 2002). They regulate the cost for insurance with premiums and excesses (Keller, 2003; Doherty et al., 2002; Seog, 2006).</td>
</tr>
<tr>
<td><strong>Thieves</strong></td>
<td>Want to steal goods (Samecki, 2003). How, what and from whom are vital questions in reality but are not addressed in this paper. Therefore, the thieves are, in this paper, only seen as external threats that cause the problem that forces the actors to handle the economical impact from the theft activities.</td>
</tr>
</tbody>
</table>

3.2.1. The actors’ movement

There are different ways that the ownership of goods transfers from seller to buyer; all from the moment the goods leave the seller’s site until the goods are picked up by the buyer in his own raw material warehouse (the VMI principle). Depending on when the ownership is passed over from seller to buyer, governs who of them buys the transport service from the Logistics Service Provider (LSP). This is the supply chain perspective of the transport network.

The LSP has a logistics network of terminals, but adjusts the actual needed freight capacity by using local haulers. The need for adjusting the capacity inside a terminal works in similar ways, by using a manning company or a work-pool system.
The antagonistic input (Ekwall, 2007) into the transport (a thief) steals a number of goods out of a certain shipment. All involved actors (goods owners, LSP, hauler and driver) hopefully have different types of insurances. Which insurance is valid is determined by which actor had the responsibility for the goods when and where it was stolen. The establishment of which actor is responsible, can, in some cases, be difficult, or even impossible to determine, due to the fact that the theft is not discovered until the shipment reaches the consignee.

The generic principle of all actors: maximize their profit, the difference between income and cost/risk in their business, will, in this specific case of a cargo theft incident, lead to the conclusion that if the theft occurred outside the company’s responsibility, then the company is not responsible for the cost of losing the goods. This is the context in which actors use the complexity within the transport network to avoid the economical impact from a cargo theft incident.

3.3. Generalisation of the old maid game strategy in logistics business

By managing one’s own company in a way that avoids the cons (cost and risk) and increases the pros (revenues and profit) is what is normally called good business. The special case of avoiding economical impact from a cargo theft incident can be illustrated based on assumptions derived from complexity theory put in the transportation network; i.e., subjective rationality in the local context. This will be shown with the old maid game, as an exemplifying strategy for the involved actors’ behaviour.

3.3.1. The old maid game strategy

The old maid game strategy is defensive to its nature and aims to avoid negative impact, hence, minimize losses. Another name for this strategy is: “the musical chairs of business.” The games old maid and musical chairs are simple to play. The important thing in both games is not to lose. In the old maid card game, the object for all players is to not be the one left with the only odd card (a queen or a jack) when the rest have no cards left. In the game of musical chairs, there is one participant more than the number of chairs. When the music stops everybody sits down and the loser is the person without a chair. There are different ways to play these two games, but the only objective is to avoid being the one left behind without a chair or with the old maid. This principle in mathematics is known as the pigeonhole principle, or, as Dirichlet’s box. The pigeonhole principle illustrates a problem solving strategy of counting argument, but which can not handle one-to-one correspondence due to that it needs more than two actors.

The principle states that given two natural numbers $n$ and $m$ with $n > m$, if $n$ items are put into $m$ pigeonholes, then at least one pigeonhole must contain more than one item. In the games of old maid or musical chairs, the relationship between $n$ and $m$ is the following: $n = m + 1$. The loser of the game is the contender $m$, which does not have an $n$.

In the context of the economical impact from a cargo theft incident, the loser is determined by pointing out the one who suffers the impact. The governing factor is who had responsibility of the cargo. Therefore, the old maid game strategy means minimizing the responsibility as much as possible without losing the income from participants in the transport network.

The importance of establishing which logistics actor is responsible for the goods when something unexpected happens to the shipment is not merely used in cargo theft incidents. The borders of liability for a certain object are equally important in every possible incident
that might lead to an economical impact on an actor. By using variants of the old maid game strategies, different logistics actors obtain a reduction in business risks through limiting their liability more than they restrict their possible income from a certain business deal. The practical transfer of risk is obtained with contracts between involved parties that expressly state each party’s liability, but, also, the potential economical compensation to a certain party fails to fulfill their commitment. Therefore, the risk transfer strategy is a vital part of the old maid game.

Case descriptions

The generalisation of the old maid game strategy in logistics business is here described with two cases. Both cases derive from experienced logistics business activities and portray two different perspectives on the old maid game strategy. Case 1 addresses impartiality towards the establishing of liability and case 2 illuminates a practical usage of the borders of liability.

Case 1: A shipping company that handles trailers and other types of freight units had a problem with claims regarding the damaging of both goods and freight units under their responsibility. The inquiry regarding these claims was conducted to establish if they were responsible. The result from these investigations was questioned by the goods or trailer owner, due to the fact that they were partially subjective in nature. The purpose was to solve this problem, and also, establish faster and better work of investigation, both regarding the actual problem and in the determination as to whether or not they were responsible for the goods when the damage was inflicted. The shipping company implemented a surveillance system based on entry and exiting control of the freight unit using multiple digital photos. These photos were saved in a database for at least six months. If someone (both internal and external) had an issue with one of the freight units, the shipping company, together with the questioner, could analyze the photos and establish what actually happened and who was responsible for it. This action has also decreased the insurance premium for the shipper company due to the fact that they have reduced their risks. A company representative (the security manager) expressed two major benefits from the surveillance system. First, the own risk for customer claims has decrease and thereby also the claims cost. Secondly, the system has demonstrated that it also helps other actors in the transport chain to simplify claims investigations and thereby reducing their claim costs.

Case 2: One of the market leading wholesalers in consumer electronics centralised their logistics activities in order to achieve effective logistics. All suppliers to the wholesaler were scheduled to deliver the ordered products to their central warehouse within a certain time-window. If they missed the time-window or something with the paperwork was wrong, then they were not allowed to unload the shipment. The wholesaler does not take over the ownership of the goods until it is unloaded in their warehouse. If the delivery in some way causes trouble to the wholesaler, then they are entitled to compensation from their supplier or from the LSP, depending on who caused the problem. This way, the wholesaler minimizes its own. In discussions with the security manager it came clear that more or less all supply risk sources (using the categorisation from Christopher et al., 2004) had been examined. This had had the effect that the wholesaler’s claim costs from inbound handling were close to zero. However, it was also expressed that their approach inevitably forced the “Old maid” to their suppliers and the LSP:s which in his belief might hamper possibilities to cooperate with the suppliers and LSP:s in other issues.
3.3.2. Analysis of the two cases

The first case describes a logistics actor that tries to establish an impartial system to simplify the investigation process when it comes to borders of liability. The second case describes the role of the consignee regarding supply risk sources. In both cases, the question of cargo liability is vital. By making sure that the borders of liability are clear and visible for all other actors (Stöth, 2004), they do all understand what risk they are taking (Waters, 2007). According to Waters (2007) this general seeking to minimize personal risks leads to the increase of a whole risk in a certain supply chain. An increased supply chain risk leads to additional risk transferring measures taken by all participants in the same supply chain. The usage of clear borders of liability perhaps reduces this increase in overall supply chain risks, but the risk transferring strategy leads to a more distinct use of the old maid game strategy in order to handle the personal business risk. This is a paradox of cooperation/competition when handling risk in transports.

4. CONCLUSIONS

The old maid game strategy is strategically defensive and aims only to avoid losses, not for generating income. The effectiveness of this strategy depends on the number of participants within the game. The basic idea is to hide in numbers. This may also be expressed as: “the more participants, the more effective the strategy.” The old maid game strategy is useful as soon as the number of actors (including insurance policies and companies) increases as a way to minimize personal business risk. The strategy may not be outspoken by each actor, but they will, to some extent, play their part in the overall business process according to the strategy. One of the key drivers of this development is the endeavour, for all involved actors, to avoid fixed cost in order to minimize this risk of ownership (Marshall, 2003). This leads to an increase in the number of actors, and they thereby increase the possibility for the old maid game strategy as a way to handle (transfer or mitigate) business risk, or more precisely, to avoid an eventual economical impact as a result from an incident during their part of the complete supply chain. With this said, the usage of a risk handling strategy like the old maid game strategy may only be described on a theoretical level. A practical way to handle business risk may very well be to establish clear and objective borders of liability in combinations with smart terms of insurance and distinct accountability towards other actors within the same business. The increasing use of enhanced liability clauses in contracts and the variation of the judgement of fulfilment of convention terms can both lead to either an increase or decrease in the usability of the old maid game strategy. The two cases used in this paper indicate the practical use of enhanced liability clauses in contracts by some actors. Both in practical and theoretical terms, this paper verifies the usability of the old maid game strategy to practically handle each individual actor’s part of the total supply chain risk in order to obtain an optimum balance between profit and risk/cost.

The result of this paper may also provide explanations for why supply chain collaboration is difficult to obtain. For those actors that perform well in the game, it is rational to live in a greater complexity as their losses can be minimized as well as their investments in improvements—at least in the short perspective. While most supply chain management literature communicates suggestions and results based on assumptions such as objectivity and rationality, complexity theory provides another set of assumptions (e.g., subjective rationality, indeterminism, complexity, emergence and self-organisation). These assumptions are more suited to a socio-technical and socio-economic context, such as supply chains, where human
beings are involved and central to the activities as well as the emergent phenomena coming from their interactions.

REFERENCES


DIFFERENCES IN STAKEHOLDER OPINION REGARDING ANTAGONISTIC GATEWAYS WITHIN THE TRANSPORT NETWORK

Daniel Ekwall

Kenth Lumsden

*) School of Engineering, University College of Borås, 501 90, Borås, Sweden
E-mail: Daniel.Ekwall@hb.se, Tel: +46 33 435 59 72, FAX: +46 33 435 40 08

**) Logistics and Transportation, Chalmers University of Technology, 412 96, Göteborg, Sweden
E-mail: Kenth.Lumsden@chalmers.se, Tel: +46 31 772 13 45, Fax: +46 31 772 13 37

ABSTRACT

The scope of logistics is relevant to all activities, from the supplier to the customer. The aim is to provide the right product, at the right time and at the right place, in spite of disturbance. To fulfil this aim a number of different stakeholders need to cooperate. One of these areas for cooperation is the reduction of problems caused by criminal activities within the logistic network. The criminal activity, which strives to illegally add (smuggling) or remove (theft) goods from a shipment, occurs at antagonistic gateways. This paper focuses on the differences in attitudes and experiences of antagonistic gateways in relation to stakeholder background and the resulting consequences. The study is descriptive and explanatory. A survey was conducted where the respondents were asked to state their acceptance of a number of relevant statements. The statements were extracted through performed research in the form of case studies and some pilot studies concerning antagonistic gateways. The respondents addressed were experts and practitioners in this logistics area. The study is based on answers from 30 companies and organizations. In the analysis these bodies were divided into six groups based on their flow chain background. The elaborated data in the form of statements from the survey was systematically presented to independent expert groups for validation. The result indicates that there is a difference in attitudes and experiences about antagonistic gateways that can only be explained by differences in stakeholder backgrounds. These identified differences have to be taken into account when designing secure gateways or introducing logistics security programs within the transport network.

Key words: Logistics stakeholder, Antagonistic gateways, Logistics security programs, Transport network, Supply chain risk
1. INTRODUCTION

This paper examines stakeholder opinions of antagonistic threats to supply chain performance within the transport network. These threats can primarily be divided into two categories, abuse of the system or theft from the system. The terrorist attacks against the World Trade Center in 2001 brought much needed attention to the security aspect of logistics. This attention is the source for many of the security programs (CSI, C-TPAT, FAST, ISPS etc.) (DHS-web, 2007) that have been developed in recent years in order to make the global flow of goods more secure.

1.1. Background

The increasing trend of globalisation in the world has led to an increase in logistic activity. The process of shipping goods around the world is long and complex (Schary and Skjott-Larsen, 2001). The international trading system is dependent on the effective transport of these goods. These transports have become more and more vulnerable. Christopher and Lee suggest that the increased vulnerability in supply chains is a result of the drive towards more efficiency, which in turn increases vulnerability from disruptions or disturbances (Christopher et al, 2004 - a). According to Svensson (2000) it “is vulnerability defined as the existence of random disturbance that lead to deviation in the supply chain of components and material from normal.” The outcome of this disturbance should also have a negative effect on the companies involved. (Svensson, 2000) This definition contains two difficulties; namely, “random disturbance” and “from normal.” The term random disturbance indicates that the focal company does not control the change, while the term from normal indicates that there is such a thing as a normal or scheduled situation.

This vulnerability can in many cases be described as “unwanted effects” in the supply chain caused either by internal or external forces that create disturbances larger than the supply chain is designed to handle. The disturbance can be either unintentional or deliberate, legal or illegal. There are basically two types of illegal and antagonistic threats to logistics, theft/sabotage and smuggling. The theft/sabotage problem is aimed directly at logistics activities, while smuggling abuses the logistics system for illegal purposes. The reasons behind these problems, as well as the different countermeasures implemented to prevent the occurrence of such problems can vary from case to case. According to Mayhew (2001) conducting a regular comprehensive risk vulnerability audit is a good way to minimize the risk for supply disruption.

There are calculations that estimate that the real numbers for the cargo theft in official reports are either grossly underestimated or overestimated (Gips, 2006). Gathering accurate numbers for cargo theft losses is difficult and in many cases impossible, due to limited reporting by the transportation industry and the lack of a national law enforcement system requiring reporting and tracking uniformity (ECMT, 2001). Despite these figures, cargo theft has generally had a low priority status in most countries and it is often perceived as the cost of doing business (EC, 2003). The introduction of illegal products in the legal transport network is considered a serious problem. In order to bring counterfeit products from the production site to the end user, the products must (in general) cross several national boundaries, as well as intellectual property legislation. The counterfeiting business evolves constantly within current trends and technology (EC-web, 2005). The production and distribution of illegal products is preformed
under the risk of detection. This environment leads to a different and diversified design of the supply chain. The location of the production facilities is subject to the risk of discovery. Illegal production units are typically placed where the risk for detection is low. In combination with the normal legal (white) business problem of where to produce products, different types of costs and quality aspects emerge. The illegal products are then distributed by using the same trade routes and port activities as legal logistics (Naylor, 2004). The most common countermeasure taken against smuggling is the inspection of cargo carriers when they cross any national border.

1.2. Research question

All stakeholders have different views and commitments in the supply and transport chain. In this study the approached research questions are based on these circumstances. The first question (RQ1) hypothesizes that these differences imply that different stakeholders have different views and opinions about theft and smuggling as threats towards their logistics business. The second question (RQ2) will extend this by suggesting that these differences can be linked to the attitude towards introducing logistics security programs.

2. FRAME OF REFERENCE

2.1. Supply chain risks and transport networks

The scope of logistics pertains to all activities from supplier to customer to provide the right product at the right time and place (Christopher, 1998). To be successful, all aspects concerning operations and information need to work together and be coordinated. The different blocks in a supply chain can literally be located throughout the world and connected through the use of transport networks. In time, the transport network affects costs, and if used smartly it can even increase the value of the product (Lambert et al., 1993). The transport network aims to fulfill the need for transport of goods in the supply chain. The consignor and the consignee shall be seen as parts in many different supply chains.

According to Christopher and Peck (2004), risk sources for a supply chain can be divided into three categories; internal, external and environmental. Internal risks can be further subdivided into process and control risks. External risks can be subdivided into demand and supply risks. The external risks can also be described as risks emerging from the interaction between the supply chain and its environment (Chapman et al, 2002). Sources of environmental risks are politics, nature and social uncertainties (Juttner, 2005). The five sources of supply chain risk provide only a general description of risks and from which direction they come in a supply chain. The term sources do not refer to the actual cause of the incident.

Studies of supply chain risks seldom address these different causes to risks (Christopher et al, 2004 - a, Christopher et al, 2004 - b, Juttner, 2005, Sheffi, 2001). They simply mention supply chain risk sources without talking about causes like theft, smuggling, sabotage and other criminal activities other than terrorism. Not all supply chain disruptions are caused by criminal activities, but many are. This study addresses the nature, effects and prevention of those criminal activities that allow goods to enter or exit the transport network by using antagonistic gateways.
2.2. Antagonistic gateways within the transport network

The physical flow of products through the supply chain is conducted by a transport network. These transport networks are designed to use economy of scale when moving products from consignor to consignee in a supply chain, through nodes and links (Stefansson, 2004). Transportation nodes are terminals, warehouses, harbours and airports, and transportation links are the means of connecting the nodes. Goods enter and exit the network through inbound and outbound gateways (Lumsden, 2006).

An antagonistic gateway is an informal and hostile gateway that adds or removes goods from the network. Theft (exiting) and smuggling (entering) can be seen as illegal and antagonistic business processes that are autonomous or semiautonomous and managed by perpetrators that act from a rational choice perspective (Sarnecki, 2003). When a product changes from the legal side to the illegal side or vice versa, it uses a gateway or crossover point. This gateway is chosen or created to minimize the risk of discovery, but also with regard to normal business constraints like cost, time and reliability (Ekwall, 2007).

2.3. Logistics security programs targeting security gaps

In the aftermath to the World Trade Center terrorist attack, several new security programs were launched. The purpose was to protect the international cargo flow from being abused for criminal (primarily terrorist) intentions, but without compromising supply chain efficiency. Several programs were launched by the US Customs office (DHS-web, 2007), like the Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI), the 24-hour rule, etc. The different security programs address different aspects of supply chain security, and they therefore target different parts of a transport chain. The link between all of these security programs is that they involve all parties or stakeholders in supply chain security (Sheu et al., 2006).

Before 9/11 2001 other types of security programs existed. These programs were primarily designed to address theft problems within the transport business (TAPA:s FSR and TSR etc.) (TAPA-web, 2007). The big difference between security programs before and after 9/11 is that afterwards, different (mainly US) authorities took the lead for both the development and implementation of these programs. Before 9/11, security was something that the business itself dealt with.

3. METHOD

3.1. Study outline

Using methodology triangulation (Mangan et al., 2004), this paper will focus on the differences in attitudes and experiences depending on stakeholder background in relation to antagonistic gateways. Through this perspective this survey shall be seen as one corner-stone in the validation of this thesis. The research presented here intends to represent reality by demonstrating that there is a difference in stakeholder opinion regarding antagonistic gateways in the transport network, and thereby contribution to the logistics knowledge base (Sachan, 2005). According to Näslund (2002), this means that in order for logistics academia...
to lead rather than follow practitioners, the relevance in their research needs to be extremely pronounced. According to Popper (1959), theories are only hypotheses that may not be true. The task for the researcher is to test these hypotheses empirically, and if proven wrong, remove that hypothesis from the knowledge base. This paper will focus on the differences in attitudes and experiences depending on stakeholder background in relation to antagonistic gateways and thereby strengthen the logistics knowledge base. The study is descriptive and explanatory. As a consequence this paper intends to describe and give possible explanations about the differences in stakeholder opinion regarding antagonistic gateways within the transport network.

3.2. Survey

A survey was conducted whereby the respondents were asked to provide their opinions in relation to 20 statements. Ten statements were initially formed by the researcher and tested in a discussion-like interview. The feedback from that single interview brought new angles and questions to the statements. The researcher then formed ten new statements and changed two of the old ones. The study was based on answers from 30 companies and organizations. The persons addressed were all experts and practitioners in this area. The respondents could choose one of the following four answers: agreeing “strongly”, “weakly” or “not at all” with “no opinion” as the fourth option.

Each company or organization was chosen by the researcher based on their market-leading position in their core business area relative to the research issues in antagonistic gateways. The involved personnel had job descriptions such as, security officer, claims adjuster and criminal expert. The main focus in this research is on Logistics Service Providers (LSP), and therefore they are the biggest group within this survey.

The combined answers (mean values) from all 30 companies and organizations were then presented to two different groups for comments and validation of the result. Both groups verified that the survey was a representative view of the problem of antagonistic gateways within the transport network. The two groups also verified that the combined conclusions drawn from the 20 statements, were valid for the business. Some statements were more concerned with addressing attitudes; therefore, the answers from the survey must be used in moderation.

The grouping of the stakeholders in this paper is presented in two steps. The first step was to create the intermediate groups. The groups were named cargo handlers and other stakeholders. The governing factor in the first step was the stakeholders’ practical relationship to the cargo handlers in everyday business processes. In the second step, the two intermediate groups were divided into six subgroups. The governing factors in the second step were to distinguish mutual business processes and positions within the transport network. The cargo handlers group was divided into two subgroups. Namely, Logistics Service Providers (LSP) and Ports and shippers. The other intermediate group, other stakeholders was divided into four subgroups. Namely, authorities, goods owners, insurance companies and consultants.

4. EMPIRICAL FINDINGS

The result was analysed statement by statement. The statements were grouped into three groups, due to the relationship between the different subjects that they addressed. The first group addressed the existence of antagonistic gateways and how they are used. The second
group is focused on the effects created by the antagonistic gateways within the transport network. The third group evaluated preventive methods or ideas against the usage of antagonistic gateways.

4.1. The nature of the antagonistic gateways

The first group of statements addressed the nature or extent of the two types of antagonistic gateways. The outcome from this group is presented in table 1. The answers are presented as they were given in the following way: strongly support/weakly/not at all/no opinion.

Table 1 Outcome statements regarding nature of the antagonistic gateways

<table>
<thead>
<tr>
<th>Statement</th>
<th>LSP</th>
<th>Shipper and ports</th>
<th>Authority</th>
<th>Goods owner</th>
<th>Insurance companies</th>
<th>Consultants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement 1</td>
<td>10/0/0/0</td>
<td>2/0/0/1</td>
<td>4/0/0/0</td>
<td>1/2/0/1</td>
<td>3/1/0/0</td>
<td>4/1/0/0</td>
</tr>
<tr>
<td>Statement 2</td>
<td>5/2/2/1</td>
<td>1/1/1/0</td>
<td>3/0/0/1</td>
<td>3/1/0/0</td>
<td>1/1/0/2</td>
<td>3/1/0/1</td>
</tr>
<tr>
<td>Statement 3</td>
<td>3/3/1/3</td>
<td>1/0/2/0</td>
<td>3/1/0/0</td>
<td>1/1/2/0</td>
<td>2/1/0/1</td>
<td>2/1/0/2</td>
</tr>
<tr>
<td>Statement 4</td>
<td>10/0/0/0</td>
<td>3/0/0/0</td>
<td>3/1/0/0</td>
<td>3/1/0/0</td>
<td>4/0/0/0</td>
<td>5/0/0/0</td>
</tr>
<tr>
<td>Statement 5</td>
<td>1/6/1/2</td>
<td>0/2/0/1</td>
<td>0/3/1/0</td>
<td>0/1/1/2</td>
<td>1/2/0/1</td>
<td>0/0/2/3</td>
</tr>
<tr>
<td>Statement 6</td>
<td>7/1/0/2</td>
<td>2/0/0/1</td>
<td>1/2/0/1</td>
<td>0/2/0/2</td>
<td>2/0/0/2</td>
<td>5/0/0/0</td>
</tr>
<tr>
<td>Statement 7</td>
<td>9/1/0/0</td>
<td>3/0/0/0</td>
<td>1/1/0/2</td>
<td>2/2/0/0</td>
<td>2/0/1/1</td>
<td>3/0/0/2</td>
</tr>
<tr>
<td>Statement 8</td>
<td>3/3/2/2</td>
<td>1/0/1/1</td>
<td>2/1/0/1</td>
<td>0/0/2/2</td>
<td>0/2/0/2</td>
<td>2/1/0/2</td>
</tr>
<tr>
<td>Statement 9</td>
<td>2/1/7/0</td>
<td>1/0/2/0</td>
<td>0/0/4/0</td>
<td>0/1/2/1</td>
<td>0/0/4/0</td>
<td>0/1/4/0</td>
</tr>
</tbody>
</table>

Statement 1: The transportation network is predictable depending on the flow of resources.
The use of scheduling within the transport network makes it predictable. The reasons behind this are many. The scheduling allows a network rhythm that aims at achieving efficiency within the entire network. It also makes it possible for the supply chain to plan their activities according to movement within the transport network (Lumsden, 2006). An excellent example is the scheduling of large ocean container ships. All stakeholders within the cargo handling group and the authority group agreed with this statement, but the rest of the groups did not fully agree.

Statement 2: The problem with cargo theft is increasing within the transportation network.
The combined answer to this statement is that the problem with cargo theft has increased to a minor degree. The big difference in opinion about this statement is that the cargo handlers in general believe that the increase is smaller, even if the problem hasn’t increased, while the other groups agree that it has. The official Swedish criminal statistics do not indicate an increase in theft problems (Brå, 2006). The answer to this statement clearly demonstrates that different experiences affect how a stakeholder sees the problem with antagonistic gateways.

Statement 3: The problem with smuggling is increasing within the transportation network.
The general opinion is that the problem with smuggling has increased to a minor degree. A differing opinion, however was found amongst the cargo handlers. The cargo handlers
believed that smuggling occurs in moderation, whereas the rest of the groups were of the opinion that smuggling has increased. The authorities strongly agree with this statement; however, the rest of the groups disagreed about the development. This illustrates the dilemma of smuggling. The actual extent of the problem is unknown, yet several theories have been created in order to demystify the problem.

Statement 4: The perpetrators endeavour to exploit the weakest link or spot when using antagonistic gateways to either add or remove goods.

All stakeholders, with the exception of one (a goods owner), agreed strongly with this statement. This is no surprise due to the belief that the potential perpetrator attacks the weakest link. The problem with this idea is that the potential perpetrator chooses the weakest link that he can exploit from his point of view. (Ekwall, 2007). This is evidenced through the fact that when the potential perpetrator finds and exploits a new method, place or tactic to open the antagonistic gateway, than it is also revealed to the stakeholder. The result is that this action also exposes the weakest link.

Statement 5: The majority of perpetrator cargo thefts are based locally to where the attacks occur.

The key term in this statement is “locally”. This could mean within city boundaries or an even smaller area. The cargo handlers and the authorities agreed weakly to this statement, whereas the rest were divided between weakly and not at all. The answers here indicate that perpetrator mobility, as a general statement, is on a regional level instead of local.

Statement 6: Counterfeit products are difficult to separate from legal products.

It is estimated by studies carried out by the Counterfeiting Intelligence Bureau, which is set up by the International Chamber of Commerce, which counterfeits accounted for 5 to 7% of world trade (ICC, 1997). The difficulty in differentiating a genuine product from a fake has become harder and harder in recent years (IACC, 2005). Links exist between counterfeited products, organized crime and terrorism (Lowe, 2006). This indicates that preventing the distribution of counterfeited products also prevents terrorism and other types of criminality.

The answer to this statement indeed demonstrated the differences between stakeholders. The authorities and the goods owners distinguished themselves from the rest of the groups by agreeing weakly to the statement, whereas the rest agreed strongly. The reason behind this is the fact that the goods owners together with the authorities have the required knowledge and information to differentiate counterfeit products from genuine products. One interviewee from the cargo handlers group stated in relationship to this statement, “we don’t care if the products are genuine or fake, as long as they pay us for moving them and we don’t get a penalty”. This quotation shall presumably not be seen as the general opinion among the stakeholders but it illustrates the practical reality in every day business. This statement is linked to statement 16.

Statement 7: Majority of cargo theft incidents involve goods of a lesser value (< 30.000 SEK).

The value of a stolen product can be calculated in several different ways, from market value to production cost and everything in between. The value of stolen goods is determined by insurance cost and other types of compensation between companies within the transport network. Therefore, different methods are used to establish the value. The value limit used in this statement (30.00 SEK) was chosen because it is approximately the same as a completely new trailer cover. The insurance costs associated with cargo theft incidents vary so much that it can be either larger or smaller than 30.000 SEK. The combination of these circumstances indicates two things about the value of a cargo theft incident. First, the cost for the created
damage during the incident can be costlier than the actual theft. Secondly, if the value of the stolen products is smaller than the insurance excess then it is less likely that the responsible stakeholder will report the theft. In such a case they don’t involve the insurance company in the process, which means that they don’t need to report the theft. These reasons contribute to the hidden (underscoring) statistics in official criminal statistics.

The stakeholders agreed fairly strong to this statement. This indicates that the cost for each cargo theft incident is fairly low and that the incident is less likely to be reported to the police. The statement is linked to statement 3 and illustrates one reason for a decline in official criminal statistics.

Statement 8: The will to report theft incidents has declined in recent years.

This statement is closely linked to the previous statement and demonstrates that the actual will to report thefts to the police has possibly decreased slightly in recent years. The general attitude towards this statement is weak. The goods owners is the group that claimed that their will to report thefts had not decreased. However, 7 stakeholders did not have an opinion about this statement, which indicates that this is a sensitive subject. Statement 7 and 8 together with 3 gives an interesting insight into the insufficiency of official criminal statistics.

Statement 9: The insider problem is overrated.

The relationship a potential perpetrator has with the exposed stakeholder is important for theft prevention measures as well as for counteractions of business related criminal activities. An insider normally has a better chance to plan and execute a successful theft or smuggling operation (Ekwall, 2007). The greatest source of risk for businesses is trusted insiders (Barth et al., 1998). Some authors consider insiders to be involved in approximately 60% of all losses (Tryon et al., 1997). Others claim that there are no reliable figures (Muir, 1996). This is interesting when compared to the fact that most countermeasures are implemented to reduce external theft (Beck, 2002). Internal perpetrators don’t attack randomly or in an unstructured manner, but more out of response to social and environmental factors that are present in the work environment (Tryon et al., 1997). This statement addresses just the perceived threats from insiders towards the transport network. The general belief is that the problem is a little overrated, but the authorities and insurance companies state that the problem with insiders isn’t overrated. An interesting point here is that three stakeholders in the cargo handling group believed that the insider threat is overrated. This can indicate that different organisations have different experiences with insiders.

Discussion

The old problem with theft and smuggling has not changed much in either extent or style. The problem with theft may be increasing, but the bulk of the theft incidents target low values. The perpetrator is believed to attack soft spots in the transport chain or abuse lesser secure transport routes for smuggling. The present world wide interest in anti-terrorist security programs has not directly changed the usage of antagonistic gateways. Due to the hidden statistics within this area it is likely that a change has occurred, but that the transport network stakeholders have yet to discover it.

4.2. The effects from the antagonistic gateways

The second group of statements addressed the effects or consequences of the two types of antagonistic gateways. The effects can be both economical and physical, but the main effect is the creation of disturbance within the supply chain. The flow of goods is disrupted and if this
disruption is big enough, then it will cause a domino effect of disturbance. The outcome from this group is presented (table 2). The answers are presented as they were given in the following way: strongly/weakly/not at all/no opinion.

Table 2 Outcome statements regarding effects from the antagonistic gateways

<table>
<thead>
<tr>
<th>Statement 10</th>
<th>LSP</th>
<th>Shipper and ports</th>
<th>Authority</th>
<th>Goods owner</th>
<th>Insurance companies</th>
<th>Consultants</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/4/3/0</td>
<td>0/0/2/1</td>
<td>0/2/2/0</td>
<td>3/1/0/0</td>
<td>0/0/1/3</td>
<td>1/1/2/1</td>
<td></td>
</tr>
<tr>
<td>Statement 11</td>
<td>8/2/0/0</td>
<td>3/0/0/0</td>
<td>4/0/0/0</td>
<td>3/1/0/0</td>
<td>4/0/0/0</td>
<td>3/2/0/0</td>
</tr>
<tr>
<td>Statement 12</td>
<td>0/4/6/0</td>
<td>1/0/2/0</td>
<td>0/2/1/1</td>
<td>0/0/3/1</td>
<td>0/1/3/0</td>
<td>1/2/2/0</td>
</tr>
</tbody>
</table>

The stakeholder who has the most to lose from a cargo theft incident is also the one who is most interested in preventing such an incident. This statement brings up the idea that the most risky position in the transportation chain is the one held by the consignor. The answers here were scattered in all groups with the smallest differences in the insurance and the cargo owners groups. It is possible to interpret this in such a way that everybody believes that they take the major portion of the economic risk. The interesting fact here is that the economic risk is controlled by all involved in the transport by business agreements, insurance contracts and similar activities. Therefore, as one stakeholder explained it, this question can’t be answered in a general way, although the result clearly demonstrates that the majority of stakeholders involved think that it is possible to claim that one certain stakeholder has the major portion of the economic risk.

Statement 11: The increased cost for transportation security will be paid by the end user.

To increase the security level within the transport network adds cost to the network. In the end, this extra cost will presumably and without exception be paid by the end user. As a general guideline, stakeholders agreed on this development. Five stakeholders maybe feared that their margin of profit will decrease due to increased security costs, which they indicated by agreeing weakly to this statement.

Statement 12: The fear of terrorist attacks against the transportation network is the primary drive for increasing security.

The interest in security adjacent logistics activities increased enormously after the terrorist attack against the World Trade Center and the Pentagon in 2001. This statement addresses the question, is it the fear of terrorists or is it something else that is the main motivation behind existing activities in security. The extreme here is that the authorities as a group agreed the most with this statement, whereas the goods owners and the insurance companies did not agree at all. The rest was in between those groups where the consultants are the closest to the authorities. The overall mean in this statement ends up between weakly and not at all. This indicates that the fear of terrorism is not the main motivating factor for increased security. The differences between the groups indicates that the closer a stakeholder is to the economic impact of a cargo incident, the less likely they are to fear terrorism as the cause. The authorities and the consultants are the ones that use the fear of terrorism in order to legitimate new regulations, technologies and routines within the transport business.
Discussion

The fear of terrorist attacks against the international cargo flow has become the excuse for or the reason behind several security programs in recent years. In the end, the cost of different security programs, technologies and equipment will be paid by the end user, or some stakeholder may end up with a smaller margin of profit than before. The economical effect from an incident will be controlled and determined by contracts and regulations.

4.3. The prevention of the antagonistic gateways

The third group of statements addressed the prevention of the two types of antagonistic gateways. The prevention can address either the cause of or the consequence from the usage of antagonistic gateways. The prevention method depends upon the character of the threat or the nature of the effect. The outcome from this group is presented (table 3). The answers are presented as they were given in the following way: strongly/weakly/not at all/no opinion.

Table 3 Outcome statements regarding prevention of the antagonistic gateways

<table>
<thead>
<tr>
<th>Statement</th>
<th>LSP</th>
<th>Shipper and ports</th>
<th>Authority</th>
<th>Goods owner</th>
<th>Insurance companies</th>
<th>Consultants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement 13</td>
<td>8/2/0/0</td>
<td>3/0/0/0</td>
<td>2/1/1/0</td>
<td>1/2/1/0</td>
<td>1/1/0/2</td>
<td>4/1/0/0</td>
</tr>
<tr>
<td>Statement 14</td>
<td>10/0/0/0</td>
<td>3/0/0/0</td>
<td>1/3/0/0</td>
<td>2/2/0/0</td>
<td>3/0/1/0</td>
<td>5/0/0/0</td>
</tr>
<tr>
<td>Statement 15</td>
<td>8/1/1/0</td>
<td>3/0/0/0</td>
<td>4/0/0/0</td>
<td>3/1/0/0</td>
<td>2/0/1/1</td>
<td>4/1/0/0</td>
</tr>
<tr>
<td>Statement 16</td>
<td>5/1/1/3</td>
<td>1/1/1/0</td>
<td>3/0/1/0</td>
<td>4/0/0/0</td>
<td>3/0/0/1</td>
<td>5/0/0/0</td>
</tr>
<tr>
<td>Statement 17</td>
<td>6/2/1/1</td>
<td>3/0/0/0</td>
<td>2/2/0/0</td>
<td>0/2/0/2</td>
<td>1/0/1/2</td>
<td>4/1/0/0</td>
</tr>
<tr>
<td>Statement 18</td>
<td>4/5/0/1</td>
<td>3/0/0/0</td>
<td>1/3/0/0</td>
<td>2/2/0/0</td>
<td>3/0/1/0</td>
<td>4/1/0/0</td>
</tr>
<tr>
<td>Statement 19</td>
<td>7/3/0/0</td>
<td>2/0/1/0</td>
<td>3/1/0/0</td>
<td>1/2/0/1</td>
<td>4/0/0/0</td>
<td>4/1/0/0</td>
</tr>
<tr>
<td>Statement 20</td>
<td>10/0/0/0</td>
<td>3/0/0/0</td>
<td>4/0/0/0</td>
<td>4/0/0/0</td>
<td>4/0/0/0</td>
<td>5/0/0/0</td>
</tr>
</tbody>
</table>

Statement 13: The perpetrator’s context (economic or political) is the key issue to understanding what the target is and how to prevent the potential incident.

The potential perpetrator can be described as a partly deterministically and partly rationally acting human being, or as one acting rationally on the margin (Ekwall, 2007). The statement suggests that terrorists (politically acting criminals) have other driving forces than a perpetrator, who is merely after money. The differences between both of these perpetrator archetypes can in many cases be very slim. An example of this is a cargo thief, who will use the stolen goods in a terrorist attack. The overall mean in this statement clearly indicates that the stakeholders believed that context is important. The divergent stakeholder group here were the goods owners; however, they were also a scattered group that demonstrated only a weak belief in this statement. This is most likely due to the fact that they are the least likely group to have been exposed to terrorist attacks.

Statement 14: Better employee awareness against theft and smuggling within the transportation network, will lead to fewer incidents.
Awareness among employees within the transport network about and against theft and smuggling is something that has received a lot of attention in recent years (CEN, 2006). The idea behind awareness is that employees affect each crime opportunity. And by making them aware of it, they can alter the opportunity and thereby increase the overall security level (Ekwall, 2007). In general terms, the stakeholders agreed on this belief but doubts were expressed by the authorities, insurance companies and the goods owners. The authorities and the goods owners were drawn to a weak belief in awareness and the other two groups were scattered, as some members really believed in awareness.

**Statement 15: More use of secure parking spaces both between and close to receiving terminals could reduce the risk of theft during transportation.**

The reduction of opportunity to open an antagonistic gateway is vital in crime prevention within the transport network (Ekwall, 2007). One of the least protected spots in a transport chain is when the trucks stop for any reason with cargo onboard. The Swedish road administration has requested investigations into the issue of secure parking (Dillen et al., 2006). The general opinion concerning secure parking is that it will have a theft reducing effect on road transports. In the groups LSP and the insurance companies, a smaller fraction expressed doubts that secure parking spaces will reduce the cargo theft problem. This statement shall be considered together with the first statement. It is interesting to observe that an increased protection of the supposed weak link, the parking of trucks, will not bring a reduction in the cargo theft problem.

**Statement 16: More inspections of shipments are needed to reduce smuggling goods.**

The need for more inspection of shipments is a part of several different international cargo security programs launched after the World Trade Center terrorist attack (DHS-web, 2007). One example of this is the ISPS Code that specifies how large an inspected container shall be. This fraction varies according to the current security level in that specific port (5, 20 or 100%) (ISPS, 2002). The stakeholders generally agreed with this statement. An interesting point here is that the doubt that inspection will reduce smuggling was put forward by the cargo handlers. The stakeholders, whose business processes are most affected by the increased inspection, were also the ones that had doubts about its effectiveness as a reduced smuggling method.

**Statement 17: EU regulations will enhance security level within the EU for transportations.**

In the aftermath of the 9/11 terrorist attack, the US government took a leading position in developing and expanding security regulations and programs. These programs are well known in the transport business (CSI, C-TPAT, FAST, ISPS etc.) (DHS-web, 2007, ISPS Code (2002). In recent years, the EU has focused on developing its own transport security regulations similar to the US programs, yet they are better adapted to the European situation and needs. The stakeholders in general had a fairly weak belief in transport network security gain from more regulations. The ports and shippers, together with the consultants, are the groups that believed the strongest in this statement. This is no surprise due to the fact that many of the security regulations (CSI, ISPS Code, etc.) have addresses that are presumed a breach in security in ports and the shipping business. The goods owners were the group that was least convinced. This may be for the same reason that the ports believe in regulations.

**Statement 18: Network based electronic surveillance is the future of security equipment.**

In the security business there has been a lot of recent interest in network technology as the next big thing in security equipment. Some of the security programs advocate the extended use of electronic surveillance systems and network technologies (ISPS Code, TAPA FSR and TSR etc.) (ISPS, 2002, TAPA-web 2007). This statement shall therefore be seen as linked to
the previous statement. The pattern is similar in statement 17 and 18. The stakeholders that act closest to the areas which have been addressed early in different security programs, were also the ones who believed most in the usage of electronic surveillance systems.

Statement 19: Successful security also solves safety problems in transportation.

The relationship between security and safety is easily illustrated with the basic idea in risk management. Risk is normally considered as a combination of the probability of an event and the negative consequence of that event. If the cause is an accident or unintentional action, than it is a safety problem, but if the cause is a deliberate action, than it is a security problem, even if in both cases the consequence is the same (Ekwall, 2007). This relationship opens up the possibility that successful security can also lead to better safety, or vice versa. The stakeholder agrees in general terms about this connection between safety and security within the transport network. Insurance companies strongly believe in this statement, but this may depend on whether that insurance company deals primarily with the consequences from incidents or accidents.

Statement 20: Security is also a quality aspect on the transportation.

This is the only statement that all participants agreed strongly and unanimously about. There are at least two reasons behind this. First, they believe that high quality means that the shipment arrives on time, at the right place and undamaged. According to this idea theft reduces the quality of the freight. The second belief is that different quality methods can be used to prevent theft and smuggling within the transport network. One consequence of this statement is that from a management perspective, the use of different security programs is similar to a quality program. There are several programs today that work in that way (C-TPAT, FAST, ISO 28001, ISPS Code, Stair Sec, AEO) (DHS-web, 2007; ISPS, 2002; ISO-web, 2007; Swedish custom-web, 2007; EU 2006).

Discussion

The idea that if the potential perpetrator has the option to attack the transport chain at its weakest spot they will do so, is a governing principle within security. This leads to the validity of the crime displacement theory within the transport network, and the idea that the weak spot is constantly changing positions and attributes (Ekwall, 2007). Therefore the preventive measures must always address new weak spots. An important idea to bear in mind is that security should be seen as a quality aspect in transport, in that it may solve more problems than it intended. One example of this is that one outcome of implementing the ISPS Code in ports was improvement of the working environment for dock workers. The traces of the different security programs are obvious in the answers to these statements.

5. ANALYSIS

In almost all of the 20 statements there were differences between the stakeholder groups, both on intermediate and subgroup levels. In some statements, the differences within a certain group were bigger than the differences between other groups, although the differences between the groups are evident. The different security programs that have been launched after 9/11 have targeted different parts or processes within the transport network. This development occurred parallel with the old problem of theft and smuggling. The coincidence of these two general processes is illustrated in statement 12, where some stakeholders claimed that the fear of terrorist attacks drives the transport security issue, while others (the majority) believed that
the same old problem (theft and smuggling) is the reason for security. This difference is also visible in the third group of statements. Based on the combined answers from all 20 statements it is possible to draw the conclusion that different stakeholders have different beliefs about what is the main cause/consequence from antagonistic gateways. In table 4 this relationship is presented.

Table 4 The relationship between stakeholders and the three perspectives on antagonistic gateways within the transport network

<table>
<thead>
<tr>
<th>LSP</th>
<th>Shippers and ports</th>
<th>Authority</th>
<th>Goods owners</th>
<th>Insurance companies</th>
<th>Consultants</th>
</tr>
</thead>
<tbody>
<tr>
<td>The nature of the antagonistic gateways within the transport network</td>
<td>Theft</td>
<td>Theft</td>
<td>Theft</td>
<td>Theft</td>
<td>Theft</td>
</tr>
<tr>
<td></td>
<td>Smuggling</td>
<td>Smuggling</td>
<td>Smuggling</td>
<td>Smuggling</td>
<td>Smuggling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The effects from the antagonistic gateways within the transport network</td>
<td>Economical</td>
<td>Economical</td>
<td>Economical</td>
<td>Economical</td>
<td>Economical</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The prevention of the antagonistic gateways within the transport network</td>
<td>Theft prevention and insurance</td>
<td>Theft prevention, inspection and insurance</td>
<td>Theft prevention, inspection, insurance and security program</td>
<td>Insurance, theft prevention</td>
<td>Theft prevention and reinsurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This difference in view-point is also found in other statements where the stakeholders closest to the security programs had one opinion whereas other groups had another opinion. This difference is obvious in result group 3, where the shippers and ports together with the authorities are closest to the security programs, but the insurance companies and goods owners are the ones furthest away from them. The difference in general opinion about theft, smuggling and security programs from each stakeholder group is presented in table 5.

Table 5 Stakeholder groups and their relations to theft, smuggling and security programs

<table>
<thead>
<tr>
<th>LSP</th>
<th>Theft</th>
<th>Smuggling</th>
<th>Security programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are used to problems with theft and therefore they see this as the main antagonistic gateway.</td>
<td>Are unfamiliar with this type of antagonistic gateway. Have a hard time preventing it.</td>
<td>Programs like C-TPAT and AEO have affected them together with theft prevention actions. An overall weak relationship.</td>
<td></td>
</tr>
<tr>
<td>Shippers and ports</td>
<td>Are used to problems with theft and therefore they see this as the main antagonistic gateway.</td>
<td>Are unfamiliar with this type of antagonistic gateway. Have a hard time preventing it.</td>
<td>The development of security programs has mainly addressed port activities.</td>
</tr>
<tr>
<td>Authority</td>
<td>The justice systems have a high accustomedness with this</td>
<td>The justice systems have a high accustomedness with</td>
<td>The idea behind the new type of security programs comes</td>
</tr>
</tbody>
</table>

13
<table>
<thead>
<tr>
<th>Goods owners</th>
<th>This problem.</th>
<th>From this group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are used to problems with theft and therefore they see this as the main antagonistic gateway.</td>
<td>The smuggling of counterfeited goods is a real threat and this awareness is increasing.</td>
<td>Will be affected in the future by programs like AEO, ISO 28001, Stair Sec. An overall weak relationship.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Insurance companies</th>
<th>This problem.</th>
<th>From this group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are used to problems with theft and therefore they see this as the main antagonistic gateway.</td>
<td>Do not address smuggling directly.</td>
<td>Have not been addressed directly in any security programs, so far.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consultants</th>
<th>This problem.</th>
<th>From this group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are used to problems with theft and therefore they see this as the main antagonistic gateway.</td>
<td>The awareness about this antagonistic gateway is increasing.</td>
<td>They have good knowledge about security programs and are implementing and certifying LSP, shippers and ports according to them.</td>
</tr>
</tbody>
</table>

Each stakeholder may have a different experience of different problems or issues that separates them from the other members in the same subgroup. An LSP who is forced to adopt a security program, yet has not been the target of cargo thieves in recent years is more likely to blame the fear of terrorism as the cause, than an LSP who has problems with theft. This difference in stakeholder experience is difficult to spot in this kind of research, that is why all results should be used as an indication of differences.

6. CONCLUSIONS

This paper has focused on differences in stakeholder opinion towards the existence of antagonistic gateways within the transport network. This paper shows that there is a difference in opinion among stakeholders within the transport network. These differences can only be explained by differences in stakeholder background and their position relative to the flow of goods. The recent development in the global flow of goods has been targeted by different security programs to prevent terrorists from attacking it and creating a logistics disturbance that affects the society continuance.

The development of new and additional security programs that address security issues within the transport network will bring attention to certain processes or stakeholders in the transport chain; hopefully it will also reduce the problem of antagonistic gateways. These identified differences have to be taken into account when designing secure gateways or introducing logistics security programs within the transport network.
REFERENCES


FIA (2001), Contraband, organized crime and the threat to the transportation and supply chain function. FIA International research ltd


ICC (1997), Countering Counterfeiting. A guide to protecting & enforcing intellectual property rights, Counterfeiting Intelligence Bureau, International Chamber of Commerce


Web:


The Role of Temporary Storage in the Transport Network in a Supply Chain Perspective

Daniel Ekwall¹, Håkan Torstensson²

¹: School of Engineering, University of Borås, 501 90 Borås, Sweden
   E-mail: daniel.ekwall@hb.se, +46 33 435 59 72

²: Swedish School of Textiles, University of Borås, 501 90 Borås, Sweden
   E-mail: hakan.torstensson@hb.se, +46 33 435 59 71

Abstract

Purpose – Today’s demand on high supply chain performance requires higher awareness about supply chain risks and uncertainty. The purpose of this paper is to analyse the role of temporary storage in the transport network in a supply chain perspective. The primary research question concerns the purpose or role of temporary storage and whether management of temporary storage can contribute to reducing risks and uncertainty in the supply chain.

Design/methodology/approach – Within the described framework of supply chain systems in a transport network, and the management and control of risk and uncertainty theoretical modelling has been used as a basis for logical deduction of the conclusions. The findings are then supported and verified by two case studies.

Findings – Temporary storage in transit is located between nodes in the transport network. The temporary storage function will act as a supply chain disturbance neutralizer, thereby reducing risks and uncertainty within the supply chain. The use of temporary storage also means exposing the transport for a larger theft risk. To avoid both supply chain disturbance and increased theft risk there are three types of solutions. Firstly, improved and more exact scheduling of delivery time. Secondly, availability of secure parking spaces whenever a resource needs to make a temporary stop. Thirdly and the most suggested reductive measure is to utilize tracking and tracing systems. All these reductive measures can be applied jointly, and as a combined toolbox they can contribute to reducing the risk and uncertainty in the supply chain.

Research limitations/implications – A comprehensive inventorying of appropriate methods to optimize temporary storage in transit has not been carried out. The deduced research results are based on theory and limited case study support and will primarily serve as a general guideline.

Practical implications – From a security point of view, temporary storage offers a crime opportunity, which needs to be reduced in order to achieve lower total supply chain risk and uncertainty. This paper describes the role of temporary storage in a supply chain risk context and provides guidelines related to the trade-off between security concerns and supply chain efficiency.

Originality/value – This paper illuminates the purpose and the drawbacks of temporary stops in the flow of goods within the transport network. The conditions for temporary storage in transit represent a trade-off, related to controlling different types of risk and uncertainty in the supply chain.

Keywords: Supply chain management, supply chain risks, supply chain uncertainty, temporary storage, transport network configuration, secure parking

Paper type: Research paper
Background

Cargo theft represents a value, which for the European Union area is estimated to be €8.2 billion each year. Considering all transports, it gives an average value of €6.72 per trip. About 41 percent of all incidents have occurred during the driving phase of the transport and nearly 60 percent during a stop. The two commonly used methods are either threats against the driver or tearing the canvas of the load unit. In 15 percent of the incidents, the lorry is stolen together with the goods. Another 15 percent represent hijacking and robbery (EP, 2007).

The TAPA organization, representing high-value technology cargo, estimated the worldwide loss ratio to 0.025 percent of the total revenue (revenue $307 billion and losses $77 million, respectively). Benchmark participant loss rates varied from 0.0038 percent to 0.25 percent of total revenue. The losses presented for individual modes of transport are as follows: road 74.6 percent; air 23.1 percent; rail 0.8 percent; and sea 1.5 percent (TAPA, 2006). This indicates that the risk for losses varies greatly between different modes of transport. It is no surprise that road and air together account for 97 percent of all losses. These two modes of transport are primarily used by the participants of the survey, depending on their high value goods.

The UK is considered as a risky part of the EU regarding cargo theft (EP, 2007), with an average loss per incident at €47,146. This cost has increased by 14.6 percent, compared to 2006 figures. The classification of the 2,284 recorded cases of cargo theft during 2007 was as follows: theft of lorries 51 percent; theft from lorry 28 percent; attempted theft 7 percent; hijack and attempts 4 percent; deception 2 percent; theft (other) 7 percent; warehouse 1 percent. Almost half of the stolen lorries were recovered within 48 hours (TruckPol, 2007).

Gathering accurate numbers for cargo theft losses is difficult or in many cases impossible, due to limited reporting by the transport industry and the lack of a national law enforcement system requiring reporting and tracking uniformity (ECMT, 2001). Despite these figures, cargo theft generally has had a low priority status in most countries and is often perceived largely as the cost of doing business (EC, 2003).

Cargo theft has shown a tendency to focus on lorries that are temporarily parked at roadside, often waiting for loading and unloading opportunities (EP, 2007; TruckPol, 2007). Temporary parking of this kind has increased in recent years, due to a number of reasons, including the reduced time windows available for loading and unloading that result from higher transportation frequency and the application of lean and just-in-time principles in logistics (Cusumano, 1994). At the same time, improved security measures in terminals make such temporarily parked lorries a more frequent target for criminal attacks, according to the theory of crime displacement (Ekwall, 2008).

In general, the observation can be made that temporary roadside parking serves as a temporary storage facility, bringing flexibility into the supply chain and thus reducing some of the time-related risk and uncertainty. The temporary storage provides the opportunity to exchange supply chain risks and uncertainty for transport network risks and uncertainty. The disadvantages of this exchange include wasted valuable transport time and the added vulnerability to cargo theft.

Research purpose and methodology

The purpose of this paper is to analyse the role of temporary storage in the transport network in a supply chain perspective. Can the disadvantages be avoided and at the same time the benefits of the reduced supply chain risk and uncertainty obtained? The analysis uses several sources, combining supply chain quality and risk with a view of cargo crime properties, to
address this research question, i.e. what purpose or role temporary storage has and whether the temporary storage concept can contribute to reducing risks and uncertainty in the supply chain, while controlling the vulnerability to antagonistic threats. Thus, the research methodology is based on a frame of reference comprising supply chain systems in a transport network, combined with the management and control of risk and uncertainty. Theoretical modelling has been used as a basis for logical deduction of the conclusions. The findings are then supported and verified by two qualitative case studies, addressing the temporary storage function in a supply chain perspective and a transportation network perspective, respectively.

Frame of reference

The supply chain and the transport network

The scope of logistics pertains to all activities from supplier to customer to provide the right product, at the right time and at the right place (Christopher, 1998). To be successful, all aspects concerning operations and information need to work together. The chain of companies, which co-operate to fulfil the scope of logistics, is called the supply chain. The supply chain is a network of autonomous or semi-autonomous business processes, producing physical goods or services for the customers. These processes can be carried out by one single company or by different ones. The supply chain normally has three major constituents, supplier, manufacturer and customer.

The current economic trends have rather than emphasising the need for vertical integration (e.g. economies of scale) argued for the need for specialization. This has forced large organisations to rely on partners, suppliers, consultants and other types of external firms to deliver customer value to their marketplaces. The need for coordination of all involved processes and companies to deliver this value is what Supply Chain Management (SCM) aims to satisfy. Successfully conducted SCM will achieve shorter time-to-market and flexibility to respond quicker to actual customer demand, by integration of information and material flow while keeping the costs down.

Christopher (2005) defines the supply chain as: The network of organisations that are involved through upstream and downstream relationships in the different processes and activities that produce value in the form of products and services in the hands of the ultimate customer”. The goal for all involved organisations is to provide the ultimate customer with the right product and the right time and place.

The physical flow of products through the supply chain is conducted by a transport network. Transport networks are designed to use economy of scale when moving products from consignor to consignee through nodes and links in a supply chain (Stefansson, 2004). Transport nodes are terminals, warehouses, harbours and airports, while transport links are means of connecting the nodes. Goods enter and exit the network through inbound and outbound gateways (Lumsden, 2006). The transport network affects cost and throughput time, and if used smartly it can even increase the value of the product (Lambert et al., 1993).

The different network constraints, together with the economy of scale, have generated several different transport network designs. One of the most common is the hub and spoke configuration, which achieves both effectiveness and efficiency. This system connects all nodes with the fewest possible links and maximizes space. The major disadvantage of this is normally longer lead times for delivery from consignor to consignee (Lumsden et al., 1999). To make the hub and spoke design efficient, all transport and terminal activities need to be co-
ordinated. This means that the supply chain has to adjust, to some extent, to the transport network. This scheduling gives the transport network a routine and a systematic rhythm, but inside this rhythm the transport network is always changing, i.e. locations, routes, goods, volume, etc.

Risk, complexity and uncertainty

The business risk is commonly stated as the likelihood for an adverse event combined with the economical impact of that event. The entire risk handling process is referred to as risk management. The usage of risk management tools and processes within the scope of logistics and supply chain management is defined by Norrman and Lindroth (2002) as:

Supply chain risk management is to [collaborate] with partners in a supply chain and apply risk management process tools to deal with risks and uncertainties caused by, or impacting on, logistics related activities or resources.

According to Juttner et al. (2003) supply chain risk management is defined as “the identification and management of risks for the supply chain, through a co-ordinated approach amongst supply chain members, to reduce supply chain vulnerability as a whole”.

To be successful, all aspects concerning operations and information need to work together. Juttner (2005) states that risk-taking is generally perceived as an inevitable aspect of supply chain management. At any case, the risks that exist within a certain supply chain need to be managed. Therefore, the managing of risks and threats against supply chain performance is effectuated by security and resilience in order to decrease the supply chain vulnerability.

Christopher and Lee (2004) suggest that the increased vulnerability in supply chains is a result of the drive towards more efficiency. To reduce this vulnerability, companies must identify their own internal risk but also the risk derived from collaboration and linkage with other companies (Juttner, 2005). The risk can be translated into a money loss, depending on either increasing marketability costs or increasing acquisition costs. Supply chain risk can also be seen as the consequence of uncertainty (Lalwani et al., 2006). A typical response to uncertainty and vulnerability is to create flexibility in the supply chain (Prater et al., 2001). A flexible supply chain can respond to changes in both internal and external factors that affect the performance. A supply chain with flexibility and appropriate response to changes can be regarded as a resilient supply chain. Resilience is defined as the ability of a system to return to its original state or move to a new, more desirable state after being disturbed (Christopher & Peck, 2004).

In research publications the main remedy against uncertainty and risk within the supply chain is to increase the level of collaboration between stakeholders. Supply chain collaboration has, however, proven very difficult to implement (Ekwall et al., 2008). The reasons for this are mainly overconfidence in technology, failures in establishing when and with whom to collaborate and the fundamental lack of trust between partners or stakeholders in the supply chain. Collaboration barriers are not addressed in this paper, only the risk and uncertainty within the supply chain and its relationship with the transport network.

The borderline between certainty and uncertainty is much of a greyscale in all business activities. Certainty in freight transport means that everything goes exactly (literally) according to plan, which rarely occurs. Thus all uncertainty cannot be eliminated. Uncertainty is simply a key characteristic of any economic activity (von Oetinger, 2004). Uncertainty often means risky business and unpredictability in relationships with customers, suppliers, and authorities. The need for uncertainty in business means that each actor, in one way or another, tries to control and reduce the amount of uncertainty he is exposed to. Supply chain
management is in this context described as reduction of uncertainty (Mason-Jones et al., 1998).

According to Prater (2005), the increasing use of information systems has improved the efficiency for the actors in the supply chain, but their intrinsic uncertainty has also increased at the same time. This development depends also on the increasing complexity and competition in the business. This complexity increase is caused by factors like irregular demand pattern, cost reduction, product specifications, and customer consolidation (Peck, 2005). The sources of supply chain uncertainty are closely related to the configuration of the supply chain, such as the distance between supplier and customer, but also the available resources (Wilding, 1998). This uncertainty is in many cases the same as the vulnerability caused by external or internal factors. The external vulnerability is caused by uncertainty in demand and forecasting and also the complexity of the supply chain, while the internal vulnerability is the same as problems in manufacturing (Prater et al., 2001). The uncertainty in demand is increased by the bullwhip effect, therefore reducing the bullwhip effect is one way to reduce uncertainty in the supply chain (McCullen et al., 2002).

The relationship between supply chain uncertainty and freight transport uncertainty is direct. Freight transport, even if it normally also generates small amounts of uncertainty to the supply chain, is used to reduce the supply chain uncertainty. This is achieved through the use of factors like scheduling, outsourcing of logistics activities, delivery frequency, and volume. There is often a trade-off between the cost and the performance of the supply chain where stock-holding cost and delivery frequencies are sources of uncertainty, which generate risks in the supply chain (Lalwani et al., 2006).

Risk related to supply chain systems

Supply chains can in general be described via a systems approach in logistics research. The description of the context and the boundaries of the supply chain are essential in order to understand the description of each supply chain. If each supply chain is separated into several different sub-systems, together they provide a wider understanding of both the context and the different boundaries. According to Arnäs (2007) it is useful to separate logistics and transport from each other and instead emphasize the dialectic relationship between the terms or systems. The logistics system is constituted by three structured elements/components: products, locations and facilities. The transport system is constituted by three structured elements/components: vehicles/vessels, freight and ways & terminals. The dialectic relationship between logistics and transport is illustrated in figure 1.

The joint positions (dialectic relationships) in figure 1 are the six different diagonal elements. The goods are represented in the terms product and freight, but in different perspectives. The infrastructure is also presented in two different perspectives as location and ways & terminals. The relocation of goods, using the infrastructure, is effectuated by the processes forwarding and movement (Arnäs, 2007).

This dialectic relationship provides an excellent description of the supply chain content of products and infrastructure, but it lacks the organizational element and also the wider environment, within which everything acts. Adding two additional systems, representing the organizational structure and the wider environment, to those stated above (logistics and transport) facilitates interpreting the context and boundaries for the supply chain system (Juttner et al., 2003).
The four levels are presented with elements and content descriptions. These elements and descriptions are of a general nature and shall not be regarded as decisive, more as illustrative and explanatory. Further, a description of the major risk sources and the different risk management strategies, normally used to manage and control the risk consequences, is attached to each level. The system of supply chain risks is presented in table 1.

<table>
<thead>
<tr>
<th>Level</th>
<th>Elements</th>
<th>Content description</th>
<th>Risks</th>
<th>Risk management strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Products and processes</td>
<td>Inventory and information flows</td>
<td>Negative - variance, inefficiency, lack of responsiveness, demand uncertainty</td>
<td>Substitution of information for inventory; better visibility, velocity and control</td>
</tr>
<tr>
<td>2</td>
<td>Assets &amp; infrastructure dependencies</td>
<td>Fixed &amp; mobile assets</td>
<td>Negative - loss of link or nodes factors</td>
<td>Insurance and contingency/business continuity planning</td>
</tr>
<tr>
<td>3</td>
<td>Organisations and inter-organisational networks</td>
<td>Contractual &amp; trading relationships, financial wellbeing</td>
<td>Positive and negative - financial decisions/ organisational failure</td>
<td>Contractually governed: partnering; dual sourcing; outsourcing</td>
</tr>
<tr>
<td>4</td>
<td>The wider environment</td>
<td>Economy, society and the forces of nature</td>
<td>Positive and negative - forces of nature: geological, metrological and pathological</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: System of supply chain with risk description and risk management strategies (based on Juttner et al., 2003 and Peck, 2008)

The business in general considers the risk sources at each level differently. A risk at the second level is normally considered as negative, while the same risk source may in the perspective presented at the third level imply a new business opportunity, which is normally considered positive.
The main focus of this paper is at the first and second level, which implies that risks are in general considered negative here. The great advantage of using the four levels (or subsystems) to describe the supply chain system is that it automatically provides a contextual understanding and boundaries to the problem of antagonistic threats towards logistics business.

Most logistics security programmes have addressed different parts of the second level, focusing on infrastructure risks and thereby achieving better security in the supply chain system. Programmes, like the AEO (Authorised Economic Operator) by the World Customs Organization, appear closer to the third level, due to the criminal background check (for customs crimes) for senior management of the certified company.

Acquisition practices and strategies, like single sourcing, just-in-time, or a reduction of supply base, all have the potential to create disturbances throughout the supply chain. The trust in e-procurement tools also brings additional risks to the supply chain (Giunipero and Eltantawy, 2003). All risk and uncertainty, in a supply chain perspective, will be transferred through a transport network. If designed and used wisely, the network can reduce risk and uncertainty. In terms of supply chain systems this is a good example of both how the first and second levels can co-operate in order to reduce the total risk and how the risk can be transferred from one level to another. This incorporates the possibility for a larger risk (increasing the potential impact consequence).

Risk control and security methods

As risk is a factor in all business functions and processes; attempts to minimize such risk have always been a part of doing business. However, minimizing the business risk often also leads to minimizing profit. Risk management methods usually strive to balance risk versus profit and cost. This can be compared to security, where an antagonistic threat needs to be managed by using direct or indirect preventive methods. Traditional risk management and security may appear to be one and the same, and many security practitioners use traditional risk management methods. Such methods are appropriate to simplify and analyse complex problems like security issues. Furthermore, they are useful methods for proper allocation of available limited resources to control unlimited risk sources and achieve a reduction of the total risk. Most risk management methods are based on statistics (obtained by various methods); therefore, they can give the risk manager a sense of dealing with scientific facts. Traditional risk management is derived from areas like insurance and safety. It is based on the idea that the world is mechanically predictable or deterministic. The stronger the linear relationship is between cause and effect, the better the traditional risk management approach for reducing disturbances is. For process failures, the relationship between cause and effect is normally linear while if there are deliberate actions behind the disturbance, the relationship can be very complex.

Most disturbances are not caused by deliberate action, like theft and sabotage. Otherwise the disturbance-reducing methods used in business should address criminal behaviour or dynamics of antagonism toward transport in general. This is not the case. The main types of disturbance are unintentional or process failures that occur with different degrees of predictability (ECR, 2003). Demand alteration or demand risk is different, as this type of disturbance is generated by a change in customer demand and further increased by the bullwhip effect, which is a practical phenomenon in industry and trade (Mitchell, 1923).

The causes of a disturbance, combined with its consequences, can always be described in risk terms, even if they are deliberate. The important part of risk thinking in a supply chain perspective is impact reduction or minimizing the total risk for disturbance. The stronger the
linear relationship is between cause and effect, the better the risk management approach for reducing disturbance is. The relationship between cause and effect is, for process failures, normally linear, while if there are deliberate actions behind the disturbance, the relationship is more non-linear. The causes for antagonism can be described as a spiral of inputs, processes, and feedback which explains the dynamics of antagonism. The understanding of the antagonistic dynamics is vital for an analysis of where, when and how the protector shall be present to prevent events from occurring. Security can thus be seen as intelligence, instead of equations containing probability and effect, as in risk management (Manunta, 1999). Therefore traditional risk management is more adequate for handling risks (quantifiable threats/problems), while security is better adapted for handling uncertainties (unquantifiable threats/problems) (Waters, 2007).

Transfer of ownership – transfer of risk

A major and very common risk in business relationships is the communication risk – that misunderstandings and misinterpretation occur, because of communication deficiencies. This may affect the transfer of ownership of the goods on their way from consignor to consignee, which then decides who is responsible for bearing the risk associated with the transport. One established asset in prevention of miscommunication is the Incoterms 2000, issued by the International Chamber of Commerce, ICC. Incoterms (International Commercial Terms) provide standardized terms of delivery for consignors, consignees and freight forwarders. In addition they comprise obligations for buyers and sellers, such as whether the consigner or consignee effectuates payment for the transport service, customs requirements, cargo insurance and compensation requests from the logistics service provider or carrier. The operator commissioned for the transportation has in his turn responsibility only towards the part who purchases the freight service (Stöth 2004). There has been a development in recent years to move the ownership transfer point downstream. Using Incoterms 2000 categorization this means that EXW (Ex Works, the seller makes the goods available at his premises) has become more unusual, while DDP (Delivered Duty Paid, the seller pays for all transportation costs and bears all risk until the goods have been delivered and pays the duty) is now more common. In terms of supply chain risk it implies that the customers reduce their supply risk source. This is done to reduce the overall supply chain risk, by almost eliminating the supplier uncertainty. In systems of supply chains Incoterms 2000 offer a valuable toolbox for the transfer of risk at the first and second level (cf. table 1) to the third level. If this is not possible, the risks at the first level can be exchanged for the risks at the second level. By using the different Incoterms intelligently, in combination with extended liability contracts, it is possible for actors/stakeholders to transfer their risk to another participant in the supply chain (Ekwall et al., 2008).

The function of temporary storage

The present trend of leanness and general low inventory levels, together with the outsourcing trend, imposes new demands on transport skills and functions. The lower inventory level reduces the robustness in the supply chain against disturbances. Then, in case of a disturbance, the supply chain will close down quicker and with a higher cost attached than it otherwise would have done. Therefore it is vital for every company to find a balance between inventory levels and the risk for disturbances in both in- and outbound logistics. This balance depends on factors like improved logistics and production planning, based on long-term and proactive relationships between buyer and seller. The flow of goods is scheduled by the buyer (Das et al., 1997). One big problem in both global and local sourcing is the time factor. Long
or variable lead times, combined with shipments in consolidated volumes, only increase the difficulty of reaching the right balance between inventory level and supply chain robustness. If the transaction or transport includes overseas movement, it will affect both the lead time and the variability of it, thereby increasing the risk for supply disruption. An increased distance between supplier and buyer also adds uncertainty due to longer lead time, complex transhipment procedures and potentially more transport disruptions.

Purchasing professionals have successively adopted policies and routines to reduce the impact and to prevent future incidents after a certain event already happened. These professionals used multiple supply sources and larger safety stocks. The reason was that risk stimulated the creation of safety buffers instead of improving the poor supply chain performance. The drawback of this practice is that safety stock often limits performance and also reduces the competitive advantage, by increasing the stock cost and prolonging the lead time. It is anticipated that future supply chain professionals must direct their attention toward the uncertainty caused by risks in the corporate environment. The companies, which best reduce this type of uncertainty, are the most likely to reach the goal of generating bottom-line performance. This requires that in the future the role of a supply chain professional becomes more strategic (Giunipero and Eltantawy, 2003). One concept that provides the required buffers to the supply chain and also reduces uncertainty is the temporary storage.

The function of the temporary storage is twofold. First, it is a place where the physical goods wait for a short period of time to achieve needed flexibility in relation to the scheduling of the supply chain or the transport network. Second, for legal and other reasons, cargo carriers need to park, refuel, or rest. The temporary storage is found between nodes, thus along the links in the transport network. The temporary storage close to a terminal or warehouse has an additional function as a waiting place before scheduled unloading, according to the just-in-time principle. The temporary storage function as time buffer in just-in-time distribution is closely related to the uncertainty of each transport. Normally there is a relationship between transport distance and the exact time of arrival. A longer distance (or longer transport time) means a larger uncertainty in time of arrival. This is solved by the use of time windows for delivery. These time windows are normally not adjusted according to the needs from the transport network. They are scheduled after the needs or demands from the terminal, warehouse, or a factory’s internal activity. Because of this, the transport network needs temporary storage close to certain delivery nodes. This activity can be seen as an uncertainty-reducing function in the supply chain.

The need for securing the material forwarding activity of the transport network contributes to reducing both the overall risk and the uncertainty of the supply chain. This is achieved by scheduling the supply chain needs with regard to in- and outbound logistics activity. The consignee wants the goods within a certain time-window, and the uncertainty in this delivery is the consignee’s inbound logistics risk. The consignor’s outbound risk consists of the uncertainty of the outbound gateway and the transport network process plus control and environmental risk sources. The uncertainty of the outbound logistics must meet the demand from the consignee’s inbound delivery window.

The usage of temporary storage is also affected by regulatory and legal issues. The conditions in the transport network are governed by different laws and regulations, which differ from one country to another. Within the European Union, the regulations have been co-ordinated. This harmonization of laws and regulations will probably continue in the future.

The current regulation for lorry driving acts as a restriction on working time and may be decisive for the need of temporary parking or temporary storage. It states that the driver is allowed to drive for 4.5 hours before a break, for 9 hours before day rest (a few hours extra in
some cases, twice a week), and furthermore perform other tasks for 4 hours before day rest (Swedish ordinance SFS 1992:47), so a 14-hour working day is possible. The allowed working time per week is 56 hours over 6 days, plus an additional 28 hours in other (non-driving) activities. This regulation applies for vehicles over 3.5 metric tonnes. Lighter vehicles have no limitation regarding driving hours; however, the day rest should be at least 11 hours (Swedish ordinance SFS 1994:1297).

Transport and freight security

The security of freight transport was long underdeveloped, but when terminal security has improved, theft incidents have increased between terminals (Ekwall, 2008). The need or demand for security during transport is for preventing unwanted negative disruption in the flow of goods. The general term for such prevention is transport security (EC, 2003). Transport security is consequently the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems, and workers against intentional unlawful acts (EC, 2003). The technological development as far as range and sophistication of anti-theft devices and after-theft systems is increasing rapidly. Special attention is given to different tracking systems that track the goods themselves throughout transport (ECMT, 2001). But applying different technological systems is only one part of a transport security strategy. The key issue is the successful coordination and cooperation of the actors involved in the transport. This cooperation has not become widely developed (ECMT, 2001). Further, there are different barriers in the business, such as underestimated risks from the haulers’ side, different standard in technologies, insurance companies not supporting by giving premium reductions, or lack of technical standards (ECMT, 2001). These barriers and lack of cooperation can be patched up by the use of common methods or standards in transport security. Together with the enforcement agencies, the operators’ associations provide and disseminate advice and guidance to operators, especially on safe routes, parking areas with high security, precautions to take, and appropriate equipment (ECMT, 2001).

The Transported Asset Protection Association, TAPA, aims, through its two different certification programmes, Freight Security Standards (FSR) and Trucking Security Requirements (TSR), at improving transport security. The FSR addresses mainly security issues at terminals and requires certification by an independent auditor. The FSR has three different levels, A to C, where A is the highest. The FSR specifies the minimum acceptable security standards for assets travelling throughout the supply chain and the methods to be used in maintaining those standards (TAPA-FSR, 2007). The TSR, on the other hand, addresses only security issues in road transport using lorries and is certified by self-assessment. Like the FSR, the TSR specifies the minimum acceptable security standards for assets travelling between terminals in the transport network and the methods to maintain those standards. The TSR shall be seen as a complementary programme to the FSR (TAPA-TSR, 2007). In transport security, it is important to take an intermodal approach to avoid unwanted competitive disadvantages between the various modes. The security methods also need to be internationally accepted, at least to reduce the risk of duplication or sub-optimal security solutions that may disrupt international trade (EC, 2003). In a typical intermodal transport the first and last part of the freight are transported by road, and in-between other modes of transport are used. As a consequence of this, road transport needs a temporary storage place near the intermodal terminal, if there is no waiting area inside the terminal borders.
Reducing risk and uncertainty and controlling vulnerability in the supply chain

The main function of the temporary storage concept is to act as a short time stockpile. The reasons behind this have been clarified previously in this paper, but they can be simplified by referring to both external and internal requirements in the supply chain. The supply chain’s internal demand can be illustrated by the scheduling of the transport and the delivery time by extended use of just-in-time delivery. The supply chain’s external requirements come both from the local environment (risks from criminal activities, etc.) and authorities (laws and regulations regarding transport, etc.), so risks and uncertainties emerge from both internal and external factors in the supply chain. For internal reasons temporary storage places close to the terminal reduce uncertainty by making it smoother to schedule all deliveries according to demands and needs in the receiving terminal. This also reduces the upstream risks. The demands of external authorities on temporary storage will induce regulations regarding working hours, employee safety, refuelling, customs passage, etc.

The environment surrounding the temporary storage and the supply pipeline can increase both risk and uncertainty in the supply chain. According to Sherman (1995), crime will, in the future, be six times more predictable by location than by perpetrator. It is easy to understand that predictable traffic movement of goods will attract criminals. A repeatedly used location provides desirable goods, which are however guarded to some degree. Therefore, the crime risk at temporary storage areas will, in the future, become more evident. These areas need to be secured than today and thereby both contribute to reducing the risk and uncertainty within the supply chain and avoid adding theft risk to the transport network.

Cases of temporary storage

The function of the temporary storage can be described with two different cases. The two cases take two different perspectives on this problem. Case 1 addresses the function in the supply chain perspective and case 2 in the transport network perspective. Both cases are based on qualitative case studies with the focus on finding real cases of operational usage of a temporary storage function in order to reduce both supply chain risk and transport risk.

Case 1 – temporary storage in a supply chain perspective

One of the market leading wholesalers in consumer electronics has centralised their logistics activities in order to achieve effective logistics. All suppliers to the wholesaler are scheduled to deliver the ordered products to their central warehouse within a certain time-window. If they miss the time-window or something with the paperwork is wrong, they are not allowed to unload the shipment. Therefore, each driver must plan the drive in such a way that the risk of missing the scheduled time-windows is at a minimum and that all documents are in order. The practical outcome of this is that lorries arrive early and wait close to the warehouse for their time-window, or if they are not allowed to unload, they wait close to the warehouse while the consignor corrects the paperwork. In either case, the area surrounding the warehouse (up to 2 km) has become a temporary storage area for loaded lorries. This concentration of lorries loaded with high-value products has an attractive influence on potential cargo thieves. To reduce the theft risk, the local management has decided to allow lorries to wait within the warehouse fences, but only if they are scheduled to unload during the same day.
Case 2 – temporary storage in a transport network perspective

A logistics service provider (LSP) stroke a bid deal with a new customer which would double the turn-over. The new customer is a manufacturer of high-value electronics and he is therefore focused on security within the transport chain. The customer also has high demands on accuracy and effectiveness in all goods movement. To fulfil the demands from the new customer, the LSP added more control points to achieve better control over the position of each shipment. The purpose behind this was to identify an actual track, instead of a presumed track of goods. The customer demanded that all weak spots, vulnerable to theft, be avoided. Therefore, the customer reviewed the actual security level in all LSP terminals and also the security between them. To reduce the weak spots during road transport, the LSP tried to reduce all temporary stops. These stops were before decided by each driver. The LSP scheduled all lorry movement with the customer’s goods so that all temporary stops would be avoided. The receiving terminal or the consignee was involved in such a way that they received an early warning that the shipment was on its way to be prepared to receive it directly when it arrived.

Analysis of the temporary storage function

In figure 1 the relationship between the supply chain and the transport network is illuminated. The two cases fit right into that figure, where case 1 addresses the focal company’s situation in the supply chain and case 2 shows the transport network perspective. In both cases the temporary storage is a concern for the company to either reduce its own supply risk (case 1) or reduce its customers’ supply chain disturbance (case 2). In both cases the main threat to the use of temporary storage is cargo theft. In other words, the security needs in the transport network, combined with the risk reduction in the supply chain imply less use of temporary storage by scheduling the movement. If the lorry needs to stop, due to regulations, refuelling, etc., it is only allowed to stop at secure parking spaces.

In principle there are only two valid risk management strategies for managing supply chain risk and uncertainty to obtain a satisfactory balance between profit and cost/risk/uncertainty, namely mitigation and transfer. Mitigation of risk refers to robustness against consequences, while risk transfer normally involves the use of insurance policies. The function of the temporary storage is primarily to mitigate supply chain risk and uncertainty by transferring elements of uncertainty to the transport chain/network and thereby increasing the resilience of the supply chain. In order to fulfill this objective, it is important that the risk and uncertainty directly linked to the usage of the temporary storage are also mitigated or transferred. To avoid both supply chain disturbance and increased theft risk there are three types of solutions. Firstly, improved and more exact scheduling of delivery time. Secondly, availability of secure parking spaces whenever a resource needs to make a temporary stop. The third and most suggested reductive measure is to utilize tracking and tracing systems. All of these reductive measures can work together, and as a combined toolbox they can contribute to reducing the risk and uncertainty in the supply chain.

Conclusions

This paper is an attempt to describe and assess the role of temporary storage in a supply chain perspective and its abilities to reduce risk and uncertainty. The internal need for the temporary storage is vital for the overall performance of the supply chain, regarding both cost efficiency
and shorter lead-time. This depends on the scheduling that governs the transport by managing the delivery time and place. From a security point of view, temporary storage will offer a location for crime opportunity which needs to be reduced in order to achieve control of the total supply chain risk and uncertainty.

In general, there are a number of basic methods to control risk, i.e. by elimination or avoidance, transfer, isolation, segregation, modification, reduction, protection, training, warning, supervision, rescue, and repair. The crucial risk here is cargo theft in temporarily parked lorries. Elimination of the risk means that either the lorry or the perpetrator will not be there. This can be achieved by routing and careful transport planning with exact scheduling of delivery, or by temporary storage facilities of the consignee, allowing loaded lorries or trailers to be dropped off without an extended waiting time. The use of slot-times, similar to the air traffic network, is one way to achieve that, but there are several methods and approaches for delivery scheduling, including software support from LIS – logistics information and ERP systems, genetic algorithms of operations research, and other feasible solutions.

Transfer of the risk is contingent upon the agreed transfer of ownership, the insurance situation, and whether the principles of crime displacement are applicable. Isolation, where the consequences do not affect the object studied, and segregation, where an adverse event cannot cause domino effects, may be achieved by technological means. The use of secure parking spaces whenever a resource needs to make a temporary stop, the use of hard-body lorries and trailers, intelligent locking devices, etc. contribute to the protection of the goods. Supervision and rescue may be effectuated by utilizing different types of tracking and tracing systems, which is the commonly most suggested reductive measure. Various risk control options can be applied synergically and as a combined toolbox contribute to reducing both risk and uncertainty in the supply chain.

References

Arnäs, P.O. (2007), Heterogeneous goods in transportation systems: a study on the uses of an object-oriented approach, avhandling, Chalmers


ECR (2003), Shrinkage: A Collaborative Approach to Reducing Stock Loss in the Supply Chain. ECR Europe, Brussels, Belgium

Ekwall, D. (2008), “The Displacement effect in cargo theft”. In proceedings of Nofoma, Helsinki

Ekwall, D. and Nilsson, F. (2008), "Using business complexity to handle supply chain risk: Dealing with borders of cargo liability”. In proceedings of Nofoma, Helsinki


The risk for detection affects the logistics system setup for cargo smugglers

Daniel Ekwall

*) Swedish School of Textiles, University of Borås, 501 90, Borås, Sweden
E-mail: Daniel.Ekwall@hb.se, Tel: +46 33 435 59 72

ABSTRACT

Purpose of this paper

This paper examines the differences in logistics system design depending on the legality of the supply chains. The legality of the goods/actors is a vital factor when taking the goods from point-of-origin to the end user. This paper uses different logistics theories to provide a likely theoretical explanation of how and in what way the legality of the supply chain affects logistics system setups.

Design/methodology/approach

This paper takes a macro-perspective on the differences between legal and illegal logistics activities depending on the legality of supply chains. The validation of this paper is based on three different structures: theoretical frame of reference, analysis of official reports and two different cases studies. This paper uses methodology triangulation and dual perspective to describe the interaction between illegal supply chains and the legal world’s preventing efforts. The key analytical feature for this paper is the risk for detection element.

Findings

Several supply chains use the transport network services and therefore it is not always possible to separate legal from illegal supply chains. The illegal supply chains have a unique constraint in comparison to the legal setup: the risk for detection. The detection risk factor is one of the greatest logistics constraints on the illegal flow of goods and it is in this constraint that the professionalism of the actors is found.

Research limitations/implications (if applicable)

The research is based on secondary sources like official statistics and interviews with security and customs personnel.

Practical implications (if applicable)

The triad logistics setup provides a good theoretical foundation to understand how the legal transport network is abused by criminal businesses. This paper illustrates that a filtration of information regarding the shipped products is the primary tool to use to successfully abuse the legal transport network.

What is original/value of paper

This paper uses well known theories from logistics research to both describe and explain the illegal supply chains.

Keywords: Illegal supply chain, Transport system, Transport network configuration, Cargo smuggling, Logistics system design
1 INTRODUCTION

This paper examines the differences in logistics system design depending on the legality of the supply chain. From a simplistic point of view, the supply chain can be either legal or illegal, but in reality, it is sometimes difficult to establish the legality. Actors on both sides of the law have different intentions—to either simplify the legality assessment process or make it difficult to assess to protect their supply chains. The legality of trade differs from place to place and time. This means that a certain product/service/sale can be legal in one geographical area and illegal in another. Therefore, the legality will affect the specific logistics setup for that supply chain. The market for illegal and undefined products are normally referred to as the black market, for products that both customers and authorities consider as illegal (drugs etc) or the gray market if the customers do not know or are able to verify if the product is legal or illegal. These products can be genuinely branded merchandise sold through unauthorized channels, counterfeited products or stolen products. The gray market is the main target for counterfeited products, and that market has become global during recent years (Myers, 1999). The gray market supply chain actor’s tries the hide the trail of the products whiles the black market supply chain actor’s only tries to hide the existence for the authorities. In both cases is the risk for detection a vital element.

The supply of the black market there normally accomplish by different types of cargo crimes. First we have counterfeiting of products or just copying a product and the closely related manufacturing of goods without regard to intellectual property rights, the so called pirated goods. Secondly we have smuggling and fraud as cargo crime types. These two types have both similarities and specific differences from counterfeiting products. The last general type of cargo crime is the theft of goods. All these types can be present, in different ways, at a certain cargo crime. It is likely that theft, frauds and other types of crimes are conducted between different criminal groups but in this paper that problem is not included. The gray market is subject to the same forces of supply and demand as legal ones (FIA, 2001). Everything that has been produced can be produced again by someone else. In terms of contraband, this simply means that everything can be a counterfeited product (IACC, 2005). To bring the counterfeited products from the production site to the end user (the supply chain perspective), they must cross several national boundaries (in general) and ignore intellectual property legislation. The counterfeiting business evolves constantly within current trends and technologies (EC - a). A counterfeited product is no longer possible to distinguish from genuine products only by sight (IACC, 2005). The fake products are nowadays so realistic that it is often necessary to perform a chemical analysis of the product before knowing if it is a fake (EC - b). The supply to different black markets can come from cargo crime, smuggling, counterfeiting, and product piracy. These criminal activities are attractive to organized crime groups because they combine high profit margins with lower risks than alternatives like drug trafficking (IACC, 2005). Common to these illegal supply chains is that they all use logistics activities to move products from the point of origin to the point of sale using the best possible setup to avoid disturbance in their logistics flow.

Whether a company decides to produce or acquire can be seen as a risk assessment strategy based on a cost-benefit-analysis. According to Mankiw (1992), the central principle in microeconomics that all households and firms optimize is “They do the best they can given their objectives and the constraints they face”. The optimize principle and the risk assessment strategy aims to fulfill Mankiw’s (1992) statement, namely an organisational internal profit/risk cost optimum. It is normally agreed that a larger business risk will require a larger expected profit, but in reality, different people risk apprehension (Cleary et al., 2006).
Normally the business risk is referred to as the likelihood combined with the economical impact for a certain negative incident/source (Wang et al., 2000). The business risk can thereby be regarded as a cost (risk cost), and consequently be understood with the same tools and theories as all other costs (Colbert, 1991; Doff, 2008). The search for minimizing personal business risk has always been a part of doing business (Waters, 2007). Risk management is, therefore, the pursuit for the optimum balance between potential profit and risks (Doff, 2008). This means that risk management includes all activities that are normally referred to as management (Hardy, 1999). The three terms security, risk management and crime prevention are often considered similar and always work together (Manunta, 1999). This idea suggests that security and risk management are good (from an ethic point of view) because they reduce crime; thus more or better security or risk management will reduce problems with crimes. The problem here is that what a crime is defined by a law, according to the principle “no crime without a law”, while security or risk management has no philosophical attachment to the law. This means that people on both sides of the law can have better or worse security or risk management and that security and risk management are not necessary against crime. This result in that the pursuit for the internal profit/risk cost optimum can be found on both sides of the law and in this philosophical presumption is the dynamics in the relation between preventive and exploit forces found.

The risk profile of a certain business is reflected in the minimum margin of profit required for someone to realize the transaction. This paper uses the idea of the economical man to describe the differences between legal and illegal logistics system setups, but it is also important to remember that there may be reasons other than economical ones behind the decision to conduct trade in three stages of legality (legal, illegal, and undefined). In short, the theory states that every person shall be seen as a rational person who makes decisions about potential business transactions, keeping in mind the relationships between the benefits transactions may bring or the troubles and risks that may result. With this said, rational people think at the margin (Mankiw, 1997), which may include more than economic elements. Buyers of illegal products are everywhere (Johns et al., 2003). What is legal in one country may be illegal in another one. For cigarettes, is it estimated that 6-8.5% of the total consumption is supplied by smuggling (Joossens et al., 1998) This leads to the possibility that the actors in smuggling can be legal companies trying to access a market that, for them, is prohibited. According Antonopoulos (2007), discourse about the gray market is filled with the idea of a criminal underworld to separate it from the legal/normal upper-world. In reality, it is difficult to establish the underworld/upper-world image.

2 METHOD

2.1 Research question

This paper analyses the similarities and differences in the setup of logistics systems with respect to the legality of the supply chain. Thus, if the legality of the supply chain is questionable (to different extents), then there should be differences in the logistics setup depending on the detection risk. This paper uses different logistics theories to provide a likely theoretical explanation of how and in what way the legality of the supply chain affects logistics system setups.
2.2 Research approach

Using methodology triangulation (Mangan et al., 2004), this paper focuses on the differences in logistics system design depending on the legality of the supply chain. Such differences should be found in the different perspectives on the balance between constraints and risk for disturbances. In this paper, the risk for disturbance in an illegal supply chain is the same as for a legal supply chain combined with the risk for detection. The validation of this paper is based on three different structures: the frame of reference, the analysis of official reports of illegal trade activities based on the framework, and two different cases of illegal usage of the legal logistics setup. This provides a methodology triangulation, which gives a basis to the credibility of this paper (Mangan et al., 2004). The research presented here intends to represent reality by demonstrating the difference in logistics system design, depending on the legality of the supply chain, and thereby the contribution to the logistics knowledge base (Stock, 1997). This relevance of this paper is twofold: first to demonstrate that common logistics theories are valid for cargo smuggling operations as well, thereby further validating these theories; and second, to point out how the risk for detection is the prime component to understanding the prevention of cargo smuggling.

This paper takes a macro-perspective on the differences between legal and illegal logistics activities as a result from the legality of the supply chain. On a theoretical level, the separation between legal and illegal supply chains is easy to accomplish, but in reality, the separation depends on specific information (ownership, local legislation, quantity, patents, material, receiver, shipper etc.). The difficulty with interpreting all the information and then determining the legality of the supply chain can be referred to as the detection risk. The preventive measures increase this risk, while the actors in the illegal supply chains want the detection risk as low as possible. Therefore, the detection risk is decisive for the logistics system setup in an illegal supply chain. This paper uses this difference between legal and illegal supply chain as the decisive factor that governs the differences between logistics system setups. The research in this thesis follows the tradition in logistics to use a system approach when answering research questions (Aastrup et al., 2008; Hellström, 2007; Gammelgaard, 1997; Gammelgaard, 2004). The “total systems perspective” became the foundation for the logistics discipline to include the entire material flow in the research (Gomes et al., 1988). The system approach also implies a top-down perspective on the system. The main idea with system theory is to illuminate holistic thinking; it is based on the assumption that the whole (system) is different from the sum of all components (Churchman, 1968; Von Bertalanffy, 1969; Hellström, 2007). According to Hellström (2007), one main issue in system theory is how elements interact with other elements in the system. This paper takes this approach one step further to include the legality of the supply chain into the total system. The most important component in a system are its boundaries and the context in which it is presented (Wilson, 1990). In this paper, the context is logistics and the boundaries are the legal demarcations that will contribute to the logistics system design. This means that all the models used in this paper are from logistics or supply chain management. Insights from complexity theory guides the search for a few guiding principles that together describe the behaviour of the system (Gault et al., 1996). This paper is a first attempt at finding a few guiding principles to describe the effects the legality of the trade has on the logistics setup. The complexity theory offers a system understanding that is based on subjectivity and paradoxes instead of objectivity and rationality in interaction between actors (Macbeth, 2002). This paper aims only to be descriptive regarding the differences in logistics system design, not in explaining why certain products are considered legal while others are not.
2.3 Description of the risk for detection element

The key analytical feature for this paper is the risk for detection element that affects the logistics system setup. The risk for detection can further be said to consist of two components. The first component is the risk for detection as discovery by an actor that is not are supposed to be aware of the actions/activities. The second component is the potential consequence of detection (supply disruption, cargo confiscation, prosecution, personal sentences etc.). This paper refers the potential consequence of detection to the theory of rational choice and the economical man (cf. Ekwall, 2007; Sarnecki, 2003; Mankiw, 1997). The components on both sides of the law can be influenced, all to change the overall possibility of success, regardless if success means detecting and preventing a freight or if it means fulfilling a shipment for an illegal supply chain. The dynamic relationship between illegal and legal actors is the key feature to understand the function of the risk for detection element. The authorities try to increase their possibility of discovering and prosecuting illegal supply chain perpetrators, while the illegal supply chain perpetrators try to minimise the risk for discovery or the potential consequences from a discovery. This dynamic relationship is illustrated in figure 2.1.

![Figure 2.1: The description of the risk for detection components used in this paper](image)

The analysis of the similarities and differences in the setup of logistics systems with respect to the legality of the supply chain is based on the dynamic relationship between illegal and legal actors that are presented in figure 2.1. To understand the complexity and range of this relationship, this paper uses both description of illegal supply chain activities and two special cases of illegal supply chains or authorial preventive measures.
2.4 Data sources and their reliability

The information about illegal supply chains and logistics operations is derived from official reports and interviews with security personnel or personnel with similar assignments. This means that the illegal supply chain description is based on secondary data instead of the preferred primary data. Trustworthy institutes like the FBI, DEA, Europol and the European Commission collected the secondary data used. In some cases, the report is from a trade association, principally regarding counterfeited products. Primary data is used in the two case descriptions in this paper. These interviews are focused on understanding cargo smuggling operations. The interviews were conducted with the purpose of obtaining examples of illegal supply chains that exploit the legal transport network. The problem here is that the only examples mentioned are those that have been discovered and not those that escaped attention. This leads to the conclusion that the research presented in this paper is limited to address failed illegal supply chain activities in relationship with legal supply chain activities, with a focus on the risk for detection. Consequently, there are successful illegal supply chains that conceal their activities more effectively than the states in this paper.

3 THEORETICAL FRAMEWORK

3.1 Logistics and the market

Christopher (2005) defines the supply chain as follows: The network of organisations that are involved through upstream and downstream relationships in the different processes and activities that produce value in the form of products and services in the hands of the ultimate customer”. The goal for all involved organisations is to provide the ultimate customer with the right product at the right time and place (cf. Christopher, 1998). The market as a concept can be used as a description for all business transactions, which includes everything from the cradle to the grave (and again, with the recycling) in a product’s life. This paper uses the market as the place were the products, regardless of legality, are exchanged for money according to the theory of supply and demand. Logistics is, according to Christopher (2005), “the process of strategically managing the procurement, movement and storage of material, parts and finished inventory (and the related information flow) through the organization and its marketing channels in such a way that current and future profitability are maximized through the cost-effective fulfilment of orders.” The striving for better business deals is the practical way to maximize profitability, and according to Naylor (2004) this strive together with the general globalization trend has lead to an embedment of illegal actions within legal markets (cf. Antonopoulos, 2007). The striving for better business deals and the general globalization trend that started centuries ago has lead to an embedment of illegal actions within legal markets (Naylor, 2004). This implies that the black markets of the past have been integrated with legal transactions, and the markets today can be described as containing many shades of grey when referring to the legality of the markets as a whole (Naylor, 2004). The legal businesses are especially concerned with the problems of counterfeit branded products and theft of their own products. To increase the efficiency of detecting counterfeited products, the legal businesses use cutting-edge technologies and security actions (Sarathy, 2006).

3.2 Supply chain and logistics theories

The scope of logistics pertains to all activities from supplier to customer to provide the right product at the right time place (Christopher, 1998). To be successful, all aspects concerning
operations and information need to work together. The chain of companies that co-operate to fulfill the scope of logistics is called the supply chain. The supply chain is a network of autonomous or semiautonomous business processes that produce physical goods or services for customers (Lin et al., 1998). These processes can be in different companies or in the same company. The need for the coordination of all involved processes and companies to deliver this value is basically what Supply Chain Management (SCM) aims to solve (Samaranayake, 2005).

Managing the total or smaller parts of the supply chain to get them to work as effectively as possible requires integration of information and material flow (Samaranayake, 2005). Successfully conducted SCM will achieve shorter time-to-market and allow the flexibility to respond quicker to actual customer demand, all while keeping the costs down (Samaranayake, 2005). The purpose of the transport network is to physically move the goods within a certain supply chain to fulfill the scope of logistics. This means that the transport network only physically integrates the supply chain with the fulfilment of the supply chain’s transport demands. Therefore, several different supply chains can be present at the same time and the same place in the transport network. The logistics triad setup focuses on the relationship between consignor, consignee, and the transport fulfilment. The foundation of the logistics triad is a cooperative, three-way relationship with the movement of goods as the core (Stefansson, 2004). The logistics triad theory is illustrated in figure 3.1.

![Figure 3.1: The logistics triad (Stefansson, 2004)](image)

The usage of a Logistics Service Provider (LSP) is generally agreed to be good business behaviour. This gives the goods owner access to the LSP’s terminal network, and thereby the LSP’s economy of scale for transports, which reduces the distribution cost and increases the possible number of potential customers (Stefansson, 2004; Lumsden, 2006; Christopher, 2005). Looking at transport from a system perspective, we find that logistics is made up of several different levels. Before examining the different levels, we should comprehend the overall logistics field. A logistics system consists of links and nodes, where the nodes are geographically fixed points, such as factories and terminals, while the links are the elements connecting the nodes, i.e., the modes of conveyance. Considering the different levels of the system, we first find the flow of material. This is the cause or the reason for the existence of the whole system, the aim of which is to move material from one place to another. To be able to do this, the material flow uses a variety flow of movable resources, meaning lorries, trains, airplanes, and ships. These movable resources need infrastructures like roads, harbours, airports, and terminals (Wandel et al., 1995).
The complexity of logistics can be explained by displaying the four different flows that are always involved in logistics activities. The flows of material and resources have already been mentioned. These two flows represent the “physical” part of logistics, but the other two flows are just as necessary to make the system work, namely the monetary stream and the flow of information (Lumsden, 2006). The four flows of logistics need, as stated before, are geographical fixed constructions and infrastructure to fulfil the logistics scope. Some of the infrastructure is owned and used exclusively by one company, while others are co-owned or even owned by governments. The four flows of logistics together with the needed infrastructure can be called the five needs for logistics fulfilment.

3.3 Constraints and disturbance risk within transport system design

Different constraints and risks for disturbance within supply chain contexts affect the actual setup of each part of the transport network. This setup is designed to obtain the optimum usage of supply chain performance and to achieve both customer satisfaction and internal efficiency. The need for customer satisfaction is the demand from the supply chain on the transport network performance and layout. Internal efficiency is the way to fulfil the demand from the supply chain. This signifies that the needs from the supply chain are the most important constraint for the transport network. Historically, security and vulnerability within the global transport network were largely neglected until the terrorist attack on the World Trade Centre. The subjects of supply chain security (the superior term for all transport related security) and vulnerability are finally being given needed attention as they pertain to terrorist attacks. This vulnerability can, in many cases, be described as “unwanted effects” in the supply chain. For the illegal supply chain, detection is an unwanted effect, and therefore is the term vulnerability also valid for illegal supply chain’s logistics systems.

Juttner (2005) states that risk taking is generally perceived as an inevitable aspect of supply chain management. Taking risks is not the same as controlling and managing risk to an acceptable level. Today, risk is a factor in all business functions and processes (Cavinato, 2004). This refers to the fact that every function or process has a certain probability of not performing as planned and that there is a certain consequence attached to that probability. Risks can emerge both from within the organisation and the environment. The attempt to minimize business risk has always been a part of doing business. According to Garrett and Marshall (2003), a common risk strategy for an actor is to own only a minor part of the equipment they use. This depends mostly on the fact that the risk for ownership is transferred; this transfer of ownership can in many cases be called outsourcing. In the world of logistics and freights, many actors have specialised in different parts/functions of the global transport network. In logistics theory, this is normally described as a good way to handle the external logistics flow for a company (cf. Lumsden, 2006; Christopher, 2005; Samaranayake, 2005).

The risk management perspective of transport from consignor to consignee and the balancing of the different constraints towards the different risks for disturbance are valid for all types of trade. If the potential risk for disturbance is considered too high in a certain logistics setup or product flow, the system should alter its design to reach an acceptable level for the mix between constraints and risk for disturbance. The difference between illegal and legal supply chains can, in its simplified form, be described as a unique constraint affecting only the illegal supply chains. The unique constraint is the risk of being discovered by the authorities, thereby suffering a flow stoppage. This unique constraint should lead to a different setup of the logistics system for the illegal supply chain to fulfil its scope of logistics. Minimising the potential effects from constraints in the transport network allows the different illegal supply
chairs to obtain better illegal business deals. According to Naylor (2004), the aspiration for better business deals together with the general globalization trend has led to an embedment of illegal actions within the legal markets. This development should therefore be visible in the global flow of goods, but illegal logistics system setups should differ from the normal (legal) setup depending on the risk of detection.

### 3.4 Detection of illegal supply chain

To increase the efficiency of detecting counterfeited products, legal businesses use cutting-edge technologies and security actions (Bolon, 2005; Sarathy, 2006). The tested technologies are organic DNA, retinal scans, holographic labels, and RFID tags (Berman, 2008). Technologies used for securing the identity of the product need to be tamper-proof. The RFID technology is not secure, but organic DNA has thus far shown good abilities on that feature (Zimmerman, 2004). These technologies aim at identifying the product as a unique entity by means of information in different shapes. The more data that needs to be consistent, the harder it is to get away with the usage of false data. It has also been suggested that customers should be educated on more easily distinguishing a fake from an original (Bolon, 2005). To do this, customers need evidence (serial numbering systems, etc.) or strong knowledge of the product. Using valuable (more expensive or rarer) materials instead of common (cheaper or easier accessible) ones may make it more difficult to counterfeit products (Hilton, 2000).

The problem with cargo crimes is complex, and depending on which type of cargo crime needs to be prevented, different methods have different impacts on the problem. The positive consequence of the “war against terrorism” is that regular cargo crimes have become harder and riskier to accomplish (Littman, 2003). For legal businesses, the AEO (Authorised Economic Operator), C-TPAT (Customs-Trade Partnership Against Terrorism), CSI (Container Security Initiative) etc. are seen as both a global supply chain headache and a business opportunity, depending mainly on the risk for thefts and counterfeiting of products for that company (Holmes, 2004). One common denominator is the use of information both to detect illegal products inside legal logistics and flows of purely illegal products. Regardless of which side of the law a businesses is on in a produce/acquire situation, the practical realization of the business needs logistics activities. The design of these activities varies with the legality of the trade.

### 4 EMPIRICAL FINDINGS

#### 4.1 Descriptions of illegal supply chains

The supply of a typical black market (both authorities and customers knows that the product is illegal) can be illustrated with the illegal smuggling of cocaine to USA. The illegal drug supply chains come mainly from South America. This depends on that the raw material, coca leaf, is grown there. The smugglers use land, sea, and air routes to get past US authorities. The whole distribution of cocaine is controlled by Colombian-based organized crime, but in recent years it has started to cooperate with Mexican criminals to streamline the logistics and share the risks. The Colombians have organized their operations in a business-like manner, creating cells for special purposes like warehousing or transport (DEA webpage). According Bouchard (2007), the illegal drug markets are best understood as having high adaptation and great resilience to always supply their products to the end user. This resilience and adaptive
ability is clearly found in the logistics system setup and can be understood and explained with the concept of risk for detection presented in this paper.

The supply of a typical gray market (only authorities know that the product is illegal) can be illustrated with the illegal smuggling of counterfeited products. The gray market involves the diversion of goods from legitimate supply chains (Huang et al., 2003). The only distinction is the risk for discovery from the authorities or the company whose products are copied. This diversity leads to a different design of the supply chain. The location of the production facilities is subject to the risk of discovery. Normally, counterfeited production units are placed where the risk for detection is low combined with the normal business problem as different types of costs and quality aspects. An counterfeited supply chain uses the freight routes and port activities in the same way as legal supply chain does. Among the receiver countries, Europe and the US are favourites, just as Africa is the favourite for transit activities. Confiscated products that have not been produced in Africa, like jewellery and CDs, show this, because the African market does not have the ability, in general, to buy that type of product. Countries in Central and South America act like magnets for counterfeited products. Purchases of counterfeited goods to launder money occur in larger numbers there than anywhere else in the world (EC - b). Large stocks of illegitimate products are easily shipped from parts of South America to Central America, where they are big consumers of that type of product. Organized crime also uses Central America as the base for shipments of illegitimate goods to North America. The situation in Europe makes it the most lucrative market for counterfeited products. The types of confiscated goods at the external borders of the EU are different from other places in the world. This indicates that the dealers of counterfeited products adjust products to each market’s special condition. They look at the fashion, culture, and buying habits of individual countries (EC - b).

Both types of Illegal supply chains use the international flow of containers to transport their products all over the world, regardless if the product is counterfeited or an illegal drug. Criminals try to delude customs’ watchfulness by "breaking" their way through from the area of production to the area of supply, and avoiding direct paths that are well known to the authorities.

### 4.2 Cases of special interest for detecting illegal trade lines

To fully understand the innovative exploitation of legal transport and logistics operations by illegal supply chain actors, it is useful take a closer look at some cases of illegal supply chains. To achieve this understanding, two interviews were conducted with key personnel. They both had long recorded experiences of the logistics business, crime prevention, and specific markets that are closely linked to the usage of illegal activities. The interview was conducted as a conversation, while all normative discussion was forbidden during the interview. This was done with the purpose to get the interviewees to state their true opinion and experience. For the same reason, all interviewees were guaranteed anonymity so that they did not fear reprimands from their employers. The interviews were all completed with a mutual survey of the notes taken during the interview to ensure that they were representative of the interview (Mishler, 1986). The first case addresses the international supply chains of art and archaeological artefacts. This case is interesting, due to the unique combination between preventive legislation (both national and international) and the difficulty in separating genuine and legal artefacts from fakes and replicas. The second case addresses the cross border preventive measures from customs’ point of view. This case demonstrates the
differences between perpetrators characteristics and their strategies to handle the commonly admittedly high risk for detection in cross border freights.

Case 1: The trade of art and archaeological artefacts is a continually increasing problem. Every country in the world has some form of rules and regulations regarding the export of these types of goods, but very few or none have import rules. The primary supplier of artefacts today is China, though quite unwilling. China has stiff export regulations, but the margin of profit is too high for some dealers. The main route is from inland China to Hong Kong (even if it is the same country, there are still different regulations). There are artefacts made “legal” (fake paperwork of artefact’s origin) and shipped to the buyers’ market mainly in Europe and the US. The big problem with this type of illegal supply chain is that it is difficult (almost impossible) to prove that the artefacts are stolen, because the only real proof that exist is the hole in the ground from which they were dug up. From an international logistics view, the actors want to mix legal (correct documentation) and doubtful objects together in the same shipment to make it even harder to prove illegal activities.

Case 2: Swedish customs categorizes the smugglers (actors who bring illegal products into or out of Sweden) into two types: small private actors or large scale organized actors. The distinction is based on the volume in each shipment. The small-scale smuggling is easier to spot and sometimes they even lack the knowledge that they are breaking a law (in cases of counterfeited products, not drugs). Large scale smugglers have thorough knowledge about both logistics and customs routines. They try to be anonymous in the eyes of the law or use goallies and front companies as importers. If it is about counterfeited products, the pure quality of the counterfeited products is much better than those of small-scale smuggling operations. Large-scale smuggling uses Sweden on a regular basis as a transit country for the goods. When the goods are drugs, the transport route is “unnatural,” with longer dead time or re-routing of the container during transport. Even re-constructed containers or ships with secret hiding places containing drugs exist.

4.3 Case discussion

Both cases show the complexity and the difficulty of prohibiting illegal supply chains from using the legal logistics system. The first case proves two things vital for illegal supply chains: flow pollution and the importance of being able to track the goods from their source (hiding or revealing the trial depending on view-point). If the authorities cannot prove that the supply chain is illegal, it must be considered legal (cf. Sarnecki, 2003) and this reduces the risk for discovery dramatically. This is the purpose, from the illegal actor’s point of view with both flow pollution and non-existing (documented) origin. The problem with counterfeited or faked archaeological artefacts is the lack of originals with which to compare the fake. This problem makes it even more difficult to distinguish fakes from authentic artefacts. Customs does not have the expertise needed to distinguish these fakes in every customs station, but in the case of counterfeited industrial products they have more of this knowledge, including which brands and which products are more likely to be counterfeited. The second case shows a big difference between professionals and amateurs regarding illegal supply chain activities. The professional acts as the unseen link in the shipment. They pull the strings and stay out of sight from the authorities; in this way they avoid the risk for negative consequences from a discovery. Therefore, it is possible to conclude that a professional illegal actor considers the two components of the risk for detection differently than the amateur who only considers the discovery risk. This leads to the customs scouts for uncommon freight routes/content/involved companies. The general idea behind this is to scout for activities that
in some way indicate that someone for some reason gave the shipment special attention (avoid the risk for discovery) in order to slip by the authorities.

5 ANALYSIS

Earlier in history there existed stationary smuggler ports and special trade routes for illegal goods, but the economy of scale in logistics has made it more efficient and fast to conceal illegal supply chain’s goods in legal shipments. Today, the creation and use of special infrastructures for illegal supply chains are likelier to be found in drug traffic (cf. the freight routes for cocaine and heroin) than for counterfeited merchandise, but the mixture of legal products with illegal ones are a common way for abusing the international logistics system. The general trend in all logistics is the need for speed, low cost, and re-scheduling of shipments so that all involved actors may receive the highest possible profit (cf. Christopher, 2005). The possibility of distinguishing legal from illegal actors varies with the type of product, documentation, means of identification, ownership etc. Therefore, illegal supply chain transport routes with the lowest possible risk of detection (both discovery risk and consequence impact for the actor) bring goods to the market with the highest possible business opportunity, payment ability, and demand.

The example of the global flow of counterfeited goods clearly demonstrates that if the fake product is difficult to separate from a genuine one (low discovery risk and low impact consequence), there is a lesser need for a different logistics system setup. While the description of the global flow of illegal drugs has a higher likelihood for detection (low discovery risk but high impact consequence), these systems have a higher likelihood of being designed to reduce the risk of detection by authorities. This results in that the colourful expression: “the darker merchandise (from a legal point-of-view) the bigger possibility to find the flow in a special designed logistics system setup”.

5.1 The triad logistics setup in the illegal logistics activity context

When shipping the illegal product to the customers, to avoid discovery the illegal logistics service provider will normally use a regular flow and a legal logistics company. The abused forwarder may not be aware that the transport is part of an illegal supply chain. The choice of forwarder, by the illegal actors, is made in the same way as the legal business stakeholders, considering price, time, and reliability as well as the possibility for the shipment to reach the market undetected. For counterfeited products or other types of goods in which it is difficult to establish if they are legal,, illegal logistics attempts to use the legal logistics system for its transport needs. The reasons for this are threefold:

1. Cost: the economy of scale in the legal business is desirable;
2. The proportions of the legal business is desirable for geographical distribution;
3. The transfer of the detection risk to another holder solves the unique illegal business constraint of risk for detection.

In terms of logistics theory this can be explained with the theory of triad logistics setup. An illegal acting LSP can transfer the actual movement of the goods/material/products to a carrier in the same way as a legal provider. The carrier is unaware of the abuse, but still receives payment for their services. With a background in both the empirical description regarding illegal supply chains transport routs and the two cases, the illegal logistics actor’s abuse of the legal logistics system is better described by adding the function of a logistics service intermediary to the triad theory. This is shown in figure 5.1.
Ekwall, D. (2009), "The risk for detection affects the logistics system setup for cargo smugglers". Submitted to Nofoma, Jönköping

Figure 5.1: Logistics setup with a Logistics Service Intermediary (Stefansson 2004)

The model in figure 3 demonstrates that a filtration of the information flow in relation to the material flow is a key issue if the legal logistics system is going to be successfully abused by illegal business actors. The economy of scale in logistics has made it more efficient and faster to conceal illegal goods in legal shipments. The general need for speed and low cost control sets the trend in the way of doing business on both sides of the law. The highest level of logistics, the flow of material, and the difference between black and white logistics is most evident (cf. Wandel). The possibility of distinguishing illegal trade lines varies with the type of product, the documentation, and the means of identification to establish the owner of the product. Therefore, illegal logistics uses the trade route with the lowest possible risk of detection to bring goods to the market with the highest possible business opportunity, payment ability, and demand. The grey line in figure 5.2 marks the vague border of where logistics activities are undefined. The box for the LSP (in figure 5.2) contains the types of activities that a LSP performs (see figure 5.1).

Figure 5.2: The black and white logistics systems (Author)
Ekwall, D. (2009), "The risk for detection affects the logistics system setup for cargo smugglers”. Submitted to Nofoma, Jönköping

For the illegal logistics actors to abuse the full potential of the legal transport network, it is necessary for them to possess a thorough knowledge of logistics and be creative in finding new ways of concealing the delivery of goods to the right buyer. A professional illegal logistics actor (cf. organized crime) takes the role of the Logistics Service Intermediary, who can use the legal Logistics Service Provider for criminal purposes.

6 CONCLUSION

This paper has illustrated that the logistical system setup differs dependent upon the legality of the trade line or supply chain that is in focus. This effect is closely linked to the risk for detection (both the risk for discovery and the negative consequence impact for discovery) which acts as a trade barrier for illegal trade lines, and is not an element in legal trade lines. Therefore, if the actors in the illegal trade line can reduce the detection risk, they will increase the possibility to use/abuse the legal global transport network for the illegal purposes. This abuse maybe detected by the different actors in legal logistics if not, the actor is still unaware of its participating in an illegal activity and continue to receive payment for the services as if the trade would be legal.

The illegal logistics system setup adjusts according to the risk of detection. This depends on that the pursuit for the internal profit/risk cost optimum. This pursuit or governing mechanism can be found on both sides of the law and it explains the dynamic relation between preventive and exploit forces in logistics and is perceptible in the differences in logistics system setup. Or more precisely in the risk for detection element which can be described as a certain risk profile for each actor, stakeholder or shipment. The risk profile of a certain business is reflected in the minimum margin of profit required for someone to realize the transaction. The theory of triad logistics setup is a useful model to describe, in practical terms, the abuse strategy from the illegal logistics actor’s side. A filtration of information regarding the shipped products is the primary tool successfully used to abuse the legal transport network. The possibility to distinguish legal from illegal products/supply chains varies with the type of product, the documentation, means of identification, ownership, location, local legislation etc. This results in that the risk for detection element is the key feature in order to understand and describe the dynamic relationship between preventive and abusive efforts executed by the different stakeholders. The full visualisation of this relationship is found in the different logistics system setup depending on the risk for detection for illegal supply chain actors by the different law enforcement agencies.

REFERENCE


Churchman, C.W. (1968), The system approach. Dell publishing, New York


Gammelgaard, B. (1997), ”The system approach in logistics”. In proceedings of Nofoma 1997, Copenhagen


Ekwall, D. (2009), "The risk for detection affects the logistics system setup for cargo smugglers”. Submitted to Nofoma, Jönköping


Ekwall, D. (2009), "The risk for detection affects the logistics system setup for cargo smugglers". Submitted to Nofoma, Jönköping


Wang, J and Roush, M (2000), What every engineer should know about risk engineering and management. Marcel Dekker inc. New York


Frames of Thefts at Work – Security Culture and the Organization of Responsibility in Transport Networks

Bertil Rolandsson and Daniel Ekwall
a School of Education and Behavioural Sciences, University College of Borås, Borås, Sweden.
E-mail: bertil.rolandsson@hb.se
b School of Engineering, University College of Borås, Sweden

In this paper we investigate how security cultures guide the way in which employees who work within global and constantly changing transport networks understand daily risks of thefts at work. Based on qualitative interviews with terminal workers at three Swedish freight terminals and on Mary Douglas’s Grid/Group model, we elaborate theoretically on how their frames of security can be understood as dependent on the organizational context. We found that the terminal workers used a so-called industrial frame of security that promotes hierarchic organizations of security. However, a conventional industrial frame, expressed by confident workers who believed that thefts should be handled by managers who followed established routines, can be distinguished from an industrial frame expressed by discouraged workers who described unpredictable external conditions that demanded their individual responsibility. A conclusion drawn is that the differences between these industrial frames indicate that our understanding of security cultures, that is, the framing of individual responsibility and inclination to act against perpetrators, has to be based on an analysis of both the organization of work and a wider organizational context.

Security Journal advance online publication, 17 November 2008; doi:10.1057/sj.2008.4

Keywords: security culture; industrial frames; thefts; responsibility; transport networks

Introduction

After the 9/11 terrorist attacks in 2001 in the U.S.A., managing security in complex transport networks has become a major concern. In particular, there are discussions among researchers and managers about how the top management may either centralize or decentralize responsibility in order to improve the security in organizations (Port of Göteborg, 2003; Naylor, 2004; Stokes, 2007). Still, we lack the knowledge about how this responsibility is understood at work in such transport networks; that is, it has to be investigated further how work shapes employees’ inclination to see security as their responsibility.

In this paper we analyse how organizational conditions shape the way in which terminal workers within transport networks view their responsibility and organizational conditions for handling the risk of theft. The concept of frames and Mary Douglas’s Grid/Group model are used to analyse the security culture among workers at three Swedish freight terminals and how it directs their understanding of responsibility for such a daily security problem (Douglas and Wildavsky, 1983; Goffman, 1974/1986; Benford and Snow, 2000). There are
similar studies on management and occupational crime among employees (Mars, 1984; Speed, 2003). Contrary to these studies, however, our focus is on institutionalized group-specific frames of security, that is, on the management of intentional and daily threats from intruders (Mannheim, 1985; Fisher, 1997; Rolandsson, 2003). We look at how workers make sense of the relation between the organization and groups at work, and their own responsibility for security at work (cf. Hui Zhang et al., 2002). The following questions have guided us through the analysis:

- How do terminal workers describe their own and the management’s responsibility for security at work?
- How do they frame the relation between the surrounding world and their working groups in terms of security?

The term security here refers to the ability to handle intentional threats. The security problems that the workers discuss concern intruders and potential thefts of freight such as white goods, electronics, tobacco, computers, etc., rather than threats against nuclear waste transports or terrorism (Huysmans, 2006). Theft of freight is a less spectacular but a more frequent problem, described as extensive by both policy makers and the transport industry (ECMT, 2001; Ekwall, 2007). As a management problem, thefts have been estimated to represent losses of at least US$10 billion per year in the United States and US$30 billion globally (Barth and White, 1998; Gips, 2006). The importance of the problem is also illustrated by the fact that the national Chief Security Officer (CSO) at one of the companies included in this study carried out tests to assess terminal workers’ inclination to act against intruders. Recognizing the problem, however, is not enough. We still lack systematically elaborated knowledge about how this problem is perceived by employees working under different organizational conditions. This is a shortcoming, which we seek to redress with this paper.

Managing security and responsibility in freight transports

This paper focuses on the question of whether or not employees are inclined to see security as their responsibility, an issue that from a management perspective can be associated with transport networks marked by both organizational complexity and rather standardized procedures of work. At first glance, descriptions of freight passing through global networks easily make us think about a comprehensive infrastructure requiring flexible and self-governing employees (cf. Castells, 1996, 1998). Organizational complexity seems to be the rule, and transport terminals are portrayed as nodes spread worldwide, dependent on extensive transport links and staff that can handle changing connections between these nodes. This type of complex network is also described as physical flows of products that go through a supply chain, conducted within a complex network of actors and new technology (Lumsden, 2006).

Figure 1 describes such a transport network; the circles represent nodes such as terminals, warehouses, harbours and airports. The transportation links are the means that connect these nodes. Goods enter and exit the network through inbound and outbound gateways, which are illustrated by squares and arrows pointing into or out of the system (Lumsden, 2006). The number of nodes through which freight could pass before arriving at the
final gateway is extensive, and illustrates the difficulty in controlling and organizing responsibility for the security within such a logistic system (cf. Naylor, 2004).

In accordance with discussions about management of organization of work and security, self-governing individuals could be seen as one way of coping with potential risks in such transport networks – in our case, thefts (Rose, 1999; Stokes, 2007). Managers are then prioritizing as well as tackling organizational insecurity, caused by difficulties in controlling the organizational complexity, by delegating responsibility from the top to the individual employee (Rose, 2000; Roberts, 2006). By including the workers in decision-making processes as well as demanding certain results, managers aim to create responsible employees who are able to handle insecurity at work, that is, make them see security as part of their job (Mythen and Walklate, 2006; Stern, 2006).

Nevertheless, we may also point to organizational features that delimit the individual responsibility taken by the employee. Such transport networks are designed to benefit from a calculated economy of scale, by moving products within or across borders – from consignor to consignee – in a supply chain (Stefansson, 2004). The networks are expected to affect cost and throughput time, increase the value of products (Lambert and Stock, 1993) and satisfy the need for deliveries within a certain time window. Hence, freight is passed through a network that has to be well planned (Ekwall, 2007). We find demands on top-down control that motivate centralized responsibility for the production and industrial ways of working. Under such conditions, management may also see security issues as annoying and expensive disturbances in the production rather than as part of the job. In addition, expectations on predictable procedures of work defined by routines may constrain attempts to delegate responsibility to employees further down in the organization (cf. Weber, 1983; Jones and Newburn, 2002; Ekwall, 2007).

The theoretical framework – the Grid/Group model

The way in which employees understand both their own and management’s responsibility for acting against potential threats at work could also be expected to vary under different conditions. By using Douglas’s Grid/Group model, we can elaborate theoretically on such organizational conditions and associated variations in their frames of security (Douglas and Wildavsky, 1983). Even if Douglas did not talk about frames, the model is constructed for studies of how risk cultures are shaped under different organizational conditions (cf. Fisher, 1997). It enables us to distinguish how ideal typical frames of security are associated with
(1) the relation between external conditions and group identities (Group) and (2) the hierarchic structure (Grid), that is, functions and levels concerning the individual worker (Mars, 1997).

Depending on whether these Grid/Group aspects are pronounced or not, four ideal typical frames of organizational security are outlined and described in Figure 2 (Douglas and Wildavsky, 1983). Two of the frames that take shape while developing these ideal types consist of pronounced hierarchies or Grid aspects. To begin with, Authoritarian frames refers to descriptions of hierarchies where workers lack both procedures of management and a joint identity upon which to rely. Weak group identities are expressed and associated with managers who distance themselves from the shop floor and divide and conquer (Lidskog et al., 1997). Power is framed as arbitrary, executed in a way that makes the employees experience difficulties in managing their work. The workers frame the surrounding world as fatal or dangerous. In addition, they frame themselves as exploited, and express lack of responsibility, which may cause insider problems and obstruction (Mars, 1984; Engdahl, 2003).

In the second type of hierarchic or industrial frame, group identity is stronger: employees take pride in their work. A hierarchic distance between management and employees is expressed, but confidence is established through legitimate routines, roles and negotiations. The employee perceives that there is a fair set of rights, making them more inclined to take responsibility for the tasks assigned (cf. Kramer, 1999). This frame contains a strong belief in formal functions and rational problem solving. Even if repetitive industrial jobs provide perpetrators with a breeding ground for calculated crimes such features are seen as tools facilitating a secure production. As long as everyone follows the plan, the surrounding world will appear as stable. Real incidents may also be perceived as annoying disturbances in the production process rather than as part of the job (Ekwall, 2007). In addition, the identification with the group is pronounced and associated with honesty and limited insider problems. Close-knit groups of workers, however, may be connected with “shoplifting” that becomes daily routine (Douglas and Wildavsky, 1983; Engdahl, 2003).

Grid aspects are not as pronounced in the two following frames, and employees are more associated with decentralized forms of responsibility. In community frames the organization is described as closed off from the surrounding world. Douglas and Wildavsky (1983) talk about sectarian organizations, in which group identification is strong. We can also imagine

![Figure 2. The Grid/Group model.](chart)

- **Authoritarian frames**
- **Industrial frames**
- **Liberal frames**
- **Community frames**
egalitarian and strong professional groups. Employees are then framed as a community of colleagues with joint responsibility for security, with a definite team spirit and professional procedures (cf. Tilly, 2000). Employees express a strong professional identity, and if somebody breaks the rules it is the community that should investigate it (Mars, 1997; Engdahl, 2003). Members frame the surrounding world as unreliable in order to sustain unity; a suspicious attitude to external actors and claims on specific knowledge are used to emphasize their joint responsibility (cf. MacDonald, 1995).

The last and fourth frame is recognized by a lack of pronounced Grid and Group aspects (Douglas and Wildavsky, 1983; Mythen and Walklate, 2006). This is a liberal frame where we find the ideal belief in self-governed individual workers. Both the group identity and the hierarchy are described as weak, and rather than referring to strong communities or predictable hierarchic routines, employees look upon themselves as entrepreneurs with the capacity to handle uncertainty (Rose, 1999). They frame the surrounding world as a market full of risks and opportunities, and themselves as rational individuals who are capable of taking responsibility for dealing with the security problem (Mars, 1984; Lidskog et al., 1997). However, highly valued individual opportunities and the loss of group identity may cause problems, by undermining honesty within the organization (Mars, 1997). In order to increase individual responsibility, managers could therefore consider steering the employees indirectly by including them in already-defined decision-making procedures (Rose, 1999; Kemshall, 2006).

Empirical material and the context of study

We have conducted 15 qualitative interviews at three different freight terminals (five interviews at each terminal) in order to elaborate further these ideal typical frames. Each interview took 30–45 minutes. The interviews were conducted during work time, which made it difficult to lengthen the conversation. We used a semi-structured guide based on three main themes corresponding with the Grid/Group model, which still allowed us to pick up unconventional ways of framing the issue of security (Ragin, 2000). Employees were asked to look at their group identification, the organizational structure and aspects of the surrounding world (temporary employment, unidentified visitors, etc.). The interviews began with less sensitive questions about workers’ background and job, enabling us to establish a sense of trust that made it easier to go beyond formal descriptions of security and theft (Kvale, 1997).

As with many other Swedish blue-collar workers, the respondents’ context of work was marked by both formalized negotiation procedures between the employer and the union, and a Swedish labour movement that over the years had strived to increase workers’ autonomy and responsibility at work (Oudhuis, 1998). Still, most of them had pre-planned and repetitive jobs at the shop-floor level with rather limited autonomy. Furthermore, they were permanently employed, had finished Swedish gymnasium school and only two of them were women. The empirical variation was increased by differences in tasks, length of employment and age (Seidman, 1998).

The terminals they worked at belonged to two different international companies with similar security organizations. A Site Security Officer (SSO) with operational responsibility for security in the terminal area could be found. In both companies the SSO reported to the terminal manager, who was responsible for the security budget, and to their line manager in
the separate security organization. Both companies had a national CSO placed in the Managing Director’s central staff, but the company that hosts the big-city terminal in our study also had appointed regional security officers responsible for security at a smaller number of terminals. All the terminals had surveillance cameras, but the SSOs as well as the employees mentioned problems with open gates and lack of identification routines that caused problems with protecting their site.

The location of these terminals also varied: the first terminal was centrally located in one of Sweden’s biggest cities, the second terminal was located in a medium-sized city that has become a logistic hub, and the final terminal – which belonged to the same company as the second terminal – was in a medium-sized city with less transport business. In addition, they were all found along three roads in Sweden where freight thefts have been considered to be a serious problem (Ekwall, 2007; European Parliament, 2007). That said, there is a lack of official and reliable statistics covering crimes against the logistic business. The police have not compiled reported thefts of freights before 2006, and none of the companies concerned were willing to share their own statistics regarding the number of thefts in each of these three terminals. Nevertheless, the CSOs at each company considered themselves well informed and were willing to rank the three terminals’ exposure to theft. Independently, they considered the exposure to be most evident in the big-city terminal, followed by the terminal located in the city with an increasing transport sector, and finally the last terminal in the medium-sized city with less extensive transport business.

The figures from the police covering reported thefts of freight in the concerned cities during 2007 support their rankings. According to these figures, there were 73 reported attacks in the surroundings of the big-city terminal that year. The second terminal, in the city with an increasing transport sector, had 52 reported attacks. The third and last terminal was located in a city where there were 10 reported attacks. That is, the two last terminals – located in medium-sized cities and belonging to the same company – are exposed to surroundings marked by a distinct difference in the amount of reported thefts. If we consider the whole region, there were 476 reported attacks in this part of Sweden during 2007, which is a slight decrease from 2006 when 517 attacks were reported. The officials responsible for compiling the reports, however, emphasized that there are a vast number of unrecorded thefts in the region (Swedish Police Authority, 2008).

Notes on method and analysis

Our aim in this paper is to describe patterns of pronounced content and the presence and absence of certain qualities in the framings of employees (Kelle, 1995) rather than measuring the causal strength of already-defined variables (Ragin, 2000). That is, we have avoided making quantitative claims on the degree of different Grid/Group aspects. This is a qualitative study, which among other things can be motivated by the fact that the issue of the study can be perceived as sensitive; employees answering ordinary surveys about thefts could be inclined to respond in a manner that they feel is expected of them, and hence less truthfully and reliably (Seidman, 1998). By carrying out qualitative interviews, there was the opportunity to spell out questions and ask respondents to explain what they meant. That is, it became possible to go beyond formal statements and to explore and try to understand what the respondents expressed.
Even more important, however, is the fact that our method is motivated by the lack of both statistics and theoretically elaborated studies dealing with the subject. There is a shortage of research into how meaning can be ascribed to thefts at work under different conditions. We recognize that our sample does not allow us to assess the situation in the transport sector in general. But, before it is possible to test causal links or draw general conclusions we need to carry out explorative studies grounded in the empirical world (Ragin, 2000). By reflecting upon how both the context and our concepts shape security culture, we are aiming at achieving theoretically elaborated knowledge that helps us understand how problems of thefts are perceived in different ways under different organizational circumstances (Kvale, 1997). By comparing frames from different terminals, we will then also be able to reach coherent interpretations, which help us formulate grounded questions that can be useful in further studies of different security cultures (cf. Miles and Huberman, 1994).

An industrial security culture at work

Starting with a brief summary of the results, we can say that terminal workers used an industrial frame while making sense of thefts and security at work. They referred to dirty environments, intensive and repetitive jobs, and lack of communication with the management. In addition, the workers underlined the need for a hierarchically organized security. Management was said to have the main responsibility for eliminating theft and improving security. Respondents from terminals in medium-sized cities also claimed that the problem was not acute. They were confident that the risk of theft could be handled by keeping working groups stable and following security routines. However, workers at the big-city terminal described discouraging external conditions, which demanded their attention. They framed the security problem as critical, and gave examples about how they, as individuals, had intervened in order to stop thieves. Security and theft were still issues for the management, but in the industrial frame used by the big-city respondents the surrounding world was pictured as less predictable. Accordingly, in the study, there were confident workers who expressed one security frame and discouraged workers who expressed a different frame altogether. Before these differences are outlined, we will describe what the workers had in common.

Grid aspects – security as a matter of hierarchic responsibility

As mentioned, all the respondents framed their jobs as industrial occupations. They saw themselves as blue-collar workers, doing simple and repetitive tasks such as sorting packages on the assembly line, driving small trucks, loading long-distance trucks, etc. Some of them had been employed for a long time, but even if they had gained more responsibility they were still on the shop floor. Most respondents also made frequent reference to poor working environments and complained about dirt, cold and the fast pace of work. None mentioned having bad relations with the management of their terminal. However, they grumbled about the distance between themselves and the managers. Rather than describing them as people they had mutual discussions with, the respondents said that the managers only dropped by occasionally or appeared at routine meetings. These are all industrial Grid aspects that illustrate a distance between top and bottom in their organizations, which
recurred at all the terminals. One respondent from the big-city terminal even described declining contact with the bosses:

> It means that you hardly know who your boss is. He may have been here for many years without you knowing who the boss is. If you look at how it was, say, ten years ago, they were out on the shop floor, moved around and talked to almost everyone, asking them how it went and if there were any problems. That never happens today!

Still, the leadership was recurrently described as legitimate. Terminal workers expressed confidence in the formal and hierarchic organization by stressing that theft and issues of security were not primarily theirs but also the managers’ responsibility. This is especially significant for workers at the terminals located in medium-sized cities. At these terminals, the respondents’ own concerns for security were not expected to make a difference; it was not a priority in their daily work and they thought that the management knew more about it than they. In addition, they claimed to have an increasing workload that did not leave time for them to, for example, control unidentified visitors. One terminal worker expressed his opinion about who should be responsible in the following way:

> …the guy who is the boss at the terminal, because I suppose that it is he who, ehh… should have this responsibility, because I do not personally think that we should have the responsibility. I mean, we do not have time to watch other people; we got too much to do. We are only working five hours a day, and at that time we sometimes got about 20,000 packages to sort during one day. So we cannot…it feels like I do not want to take that responsibility. So it might just as well happen that somebody passes by, and then it feels like it should be my fault and I might not want to have… No, I do not…somehow I do not think it is our responsibility.

It should be mentioned that the respondents at the big-city terminal, however, were inclined to take individual responsibility for security (a difference discussed later in this paper), and that some respondents had their doubts about whether their specific manager did enough to stop recurring thefts. At all terminals, nevertheless, they expected the issue to be dealt with mainly from the top; they seemed to have confidence in the way work was formally organized and never questioned the hierarchy as such.

*Group aspects – good spirits at work and temporary staff*

The respondents also expressed group aspects fitting an industrial frame. First and foremost, they expressed a strong joint identity while moderating their complaints about poor working conditions or lack of communication. They declared that they really liked their working colleagues and that they had a good climate at work – despite a lack of feedback from the top and repetitive tasks.

This emphasis on a strong group identity also became evident when respondents described themselves as a core group distinguished from the temporary workforce that was called in during busy periods. The increasing presence of employment service companies as a whole was framed as a potential hindrance to the maintenance of acceptable routines and
organizational stability, and they also stressed that the good spirits at work could be threatened if the use of temporary staff became too extensive. It would mean that the terminals would host rising numbers of employees who were less responsible as well as less reliable in terms of efficiency and security. As can be seen from the quotation below, in some cases rather strong words were used to emphasize the anxiety the respondents felt:

No they are so shameless, and so... ehh, so I do not think this is the way... This Dell-theft was pretty planned, I believe. They knew what they could find, that is the theory we have had and discussed. After all, there are plenty of these employment service companies, and they do not have the same control over their people...

Most respondents still had confidence in how the management currently dealt with security problems, for example, by following the routines and engaging the same set of extra workforce during busy periods. This was also the way in which they framed their relations with the truck drivers; even if they came from the outside and did not belong to their group, they came on a regular basis and were therefore relied upon. Especially at the terminals in medium-sized cities the workers believed that they still worked in stable organizations. However, the quotation above illustrates the fact that there was an insider theme and a concern for employment service companies that could bring in a potential lack of control and less reliable people.

Management, routines and honest working groups

At all the terminals, respondents mentioned problems with the vast number of unidentified visitors, and demanded that the management arrange better opportunities for the organization to identify the people who appeared inside their terminals. This request was associated with a broader wish to be able to prove that they and their working groups were honest. They talked about the importance of putting up fences, using ID cards or using cameras that could help the management for surveillance of goods, etc. Pleas for better surveillance were also articulated in connection with the recurrent insider theme. As mentioned, several respondents were worried about the risk that an unreliable workforce could infiltrate their groups. They saw a more active use of, for example, cameras as a way of identifying dishonest employees who could give them and their colleagues a bad reputation.

This plea for an even more frequent use of resources such as surveillance cameras confirms that the respondents expected management to have the main responsibility for keeping the terminals secure and free from theft. One of the terminal workers declared that more efforts from the top to improve security could also limit the risk of suspicion between terminal workers:

Well, it still has to be the case that if they (the management) notice that we have a lot of thefts at work, they obviously have to inform us. After all, it can be one of us! Now... it could just as well have been me who took that sewing machine, because I do not think that anyone would react if I did. Sometimes I pick up an empty cardboard box in which there has been expensive computer paper, and I put something else in it. On such occasions I could of course have taken a proper box with paper
in it, even if they are extremely expensive, because I need paper for my computer. So, it could have been me, and therefore if they have had any problem with this they should have informed us. Even if we do not know who it is, we should not be suspicious of each other – absolutely not! If we say that I had done something, stolen something, and then I realize that they got their eyes’ open I might think that maybe I should… quit with this now!

In brief, senior management at the terminals were expected to have the main responsibility to handle security and thefts, and by taking active responsibility, the management was believed to limit insider problems among the employees. Terminal workers also emphasized the importance of stability and routines within their own group and in the organization, that is, a framing of Grid and Group aspects that corresponds with the previously mentioned industrial frame of security (Douglas and Wildavsky, 1983; Engdahl, 2003). However, we have also implied that there are differences between the terminals in the industrial framing of thefts, which are important to our understanding of how such frames guide their view of security and their responsibility.

Different frames of thefts at work

We can distinguish between an industrial frame expressed at terminals in medium-sized cities by workers with confidence in their management and strong group identification, and an industrial frame expressed at the big-city terminal by workers who were discouraged about external conditions that were problematic and demanded their individual intervention.

At one terminal located in a medium-sized city, the respondents did complain about problems with protecting the terminal from unreliable visitors coming from outside. One such problem, however, concerned a broken gate, which was perceived as a temporary problem and simple to fix. This should be compared with the situation of respondents at the big-city terminal, who did not see any opportunity to close themselves off from surrounding public spaces. They expressed a sense of frustration, associated with the location in the city centre and the constant flow of people in their surroundings. In addition, the workers at this terminal stressed the difficulties that existed with international transports, and tracing more serious thefts of freight (mostly electronics) or even of entire long-distance trucks. As illustrated in the quotation below, this frustration or discouragement was also connected with concerns about a lack of knowledge of how to handle the problems that were connected with the specific location of the terminal:

No, with some education, maybe you could, but you know how it works …You know, it is this thing with closed gates and then the road passing outside that appears to be public. We should have closed gates so that people cannot enter at all. But, that is probably not possible with a public road passing here.

The external conditions that the workers at the big-city terminal identified as problematic also recur in their descriptions of who they thought the perpetrators were. As previously mentioned, at all terminals the main reason for burglaries was said to be dishonest temporary staff or insiders. Furthermore, managers were expected to limit this problem by following certain routines and engaging the same additional workforce each time more staff was
needed. At the big-city terminal, however, the respondents also spoke about an external threat from organized criminals, with connections inside the transport sector and extremely good knowledge about transports of specific freight. These perpetrators appeared to be more difficult to handle with technology or employment routines; they were described as professionals who were difficult to stop. One respondent from the big-city terminal declared:

Well, the guys that come here, they are professionals, they are incredibly skilled at what they are doing. They’re professional thieves ehh… and they know where to go. You do not just enter the terminal anywhere and pick up three laptops in a few minutes, if you do not know where the stuff is. And how do you know that?

Some respondents also referred to, for example, junkies who easily found their way from the nearby city centre to their terminal. This, together with the idea of skilled criminals, gives a picture of unpredictable external conditions that differ from the terminals in the medium-sized cities. In particular, the idea of professional perpetrators coming from the outside did not occur among the respondents at these terminals. At one of the terminals they talked about teenagers who might be in need of immediate cash. At the other terminal the respondents referred to a well-known local thief who used to commit burglaries. Some also mentioned foreign truck drivers who occasionally could be less reliable. However, these thieves seemed to be responsible for occasional rather than systematic and professional burglaries.

Security and individual initiatives

The differences in the framing of the terminals’ external conditions were also associated with a difference in the framing of individual responsibility. At the terminals in medium-sized cities, respondents claimed that the number of thefts had gone down and they did not frame thefts as an urgent matter; the surrounding world appeared to be stable. However, all the respondents at the big-city terminal were clearly bothered about thefts and framed it as an increasing problem. Furthermore, several of the workers at this terminal had personal experiences of intruders whom they had tried to stop. One of the workers described how he had intervened in order to stop an intruder:

I chased this guy a few years ago (laughter). We got these cages, you know, where we have been storing valuable freight for several years, and we got customers that pay extra for us doing that. I saw this guy climbing over this incredibly high fence and ehh… he sees me running after him, but I do not catch up with him because he ran off over the railway and towards the city centre. The fact that I happened to see him meant that I went up to the police in order to look at pictures, but it was impossible to recognize anyone.

A clear inclination to take responsibility is expressed in this quotation. Another respondent at the same terminal even underlined the importance of being suspicious and keeping their eyes on potential suspects:

I am a little bit suspicious I guess. No, but if I see someone at the terminal I do not recognize I cycle after him and look at what he is doing and if he has any reasons to be here…
Respondents at the big-city terminal appeared to be prepared for intruders and talked about the need to confront unidentified people; asking unrecognized visitors about their identity was more or less framed as a duty. In addition, even if they could all describe the security routines at work, they emphasized that employees also had to be better at following them – for example, by closing the gate after a truck had been loaded – and felt a need to gain more education on how they could act under circumstances associated with theft.

This should be compared with the respondents at terminals in medium-sized cities who expected that most of the responsibility should rest with the management. At these terminals, workers talked about a need to improve security with IDs, vests, cameras, improved gates, etc. Such improvements could keep unauthorized visitors out, but were the managers’ responsibility and not their own. One of them even talked about the fear of being perceived as rude if he had to ask unknown people to identify themselves. A test of their inclination to confront unidentified persons that was done by the national security agent (CSO) at the company six months before our interviews, was also described as incomprehensible and appeared to have annoyed some of the respondents:

Now, we got this paper from the company’s security agent (CSO) about the fact that he had entered, picked up a sewing machine and just walked out. Well…. Help. When you think about it, people really can go in and out here without us saying anything. But, now he has told us that whenever we see a face we do not recognize we should walk up to them and ask them what they want. That does not (laugh-ter) feel good, because I mean, if you would enter the terminal and I would ask, “Excuse me, but what are you doing here?”, and then it turns out that you are the boss of the company… Do you understand, it does not feel correct; it feels strange that this would be one of my tasks.

Summing up the differences between the two terminals, we can stress that respondents at the terminals in medium-sized cities did not frame thefts as an urgent matter in the same way as workers at the big-city terminal. All the respondents referred to the managers’ responsibility, but the latter group added external conditions that were difficult to control, due to their location in one of Sweden’s biggest cities and to professional criminals. Such conditions demanded their individual responsibility, and in most cases they also had experiences of intervening themselves. At the medium-sized city terminals, burglaries were framed as rather occasional, and something that youngsters or a well-known local thief might commit. Furthermore, the framing of the issue as something they thought they were not responsible for became even clearer when they described the above-mentioned test to assess the staff’s understanding of their responsibility for security. The test was executed by a central security agent and was framed by several as a strange central initiative.

**Analysis of the industrial frames of security**

In this study, all workers mentioned industrial frames of security at work. In accordance with the Grid/Group model, they described a legitimate hierarchy and strong group identification. They wished to keep the organization and working groups honest and stable (Douglas and Wildavsky, 1983; Engdahl, 2003). Rather than referring to autonomous
individuals conducting complex jobs in an ever-changing transport network, they framed themselves as decent blue-collar workers at the bottom of the organization. They complained about repetitive tasks, bad working conditions and poor communication with the top management, which restricted their own initiatives. Furthermore, it was important to them that management followed established routines and procedures at work (Mars, 1997).

Despite the differences mentioned in the industrial frames and in the statistics over reported thefts in each city, no respondent voiced explicitly a desire to have an organization of security in which self-governed individuals replaced hierarchic top-down control (cf. Rose, 1999; Stern, 2006). Even if the big-city terminal appeared to be exposed to less controllable circumstances, the workers claimed that it was mainly the management that had responsibility for reducing the risk of theft at work. Most of them wanted to see more initiatives from the managers rather than from themselves, which underlines the importance they attached to a stable hierarchy. Accordingly, nobody associated management with, for example, an arbitrary and authoritarian power exercise that, according to the Grid/Group model, could undermine the responsibility that employees experienced. Furthermore, nobody described close colleagues – or even the union – that, according to a community frame, would be collectively responsible for security at work (Douglas and Wildavsky, 1983). As shown in Table 1, the security culture among workers consisted of clear expectations of a formal and hierarchic way of running the terminal’s security top-down.

However, there were differences in framing individual responsibility when external conditions were discussed. Respondents at the big-city terminal described a need to intervene in security matters. Based on our empirical material, we cannot say whether their inclination to take responsibility depended on inclusion in decision-making processes with the management. What we can say, however, is that the above-mentioned statistics and the CSO’s ranking support the description of their terminal as being exposed to surroundings that host more potential intruders than the other terminals. Their experiences of organized crime and their location in the city centre can be seen as reasons for workers feeling that they, in accordance with a liberal frame, had to take individual initiatives on the shop floor (Mars, 1984). Given that they wanted more education and knew about the security policy, we may also say that they combined a wish that the management should take most of the responsibility, with features of self-governed workers who conduct themselves in accordance with policies and rules in the company.

Table 1  An industrial frame of security

<table>
<thead>
<tr>
<th>Grid aspects</th>
<th>Group aspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repetitive tasks, fast pace of work and limited responsibility at the shop floor.</td>
<td>Stable organizations and working groups.</td>
</tr>
<tr>
<td>Confidence in the formal hierarchy.</td>
<td>Honest working groups.</td>
</tr>
<tr>
<td>Security managed top-down.</td>
<td>Stressing routines for, for example, surveillance, closing gates and temporary staff.</td>
</tr>
</tbody>
</table>
Confident and discouraged terminal workers – some conclusions

Consequently, we are facing security cultures marked by two different industrial frames of the problem. To begin with, respondents from the terminals in medium-sized cities were confident about the opportunities to limit the problem. They stressed that the management had the responsibility and that an existing organizational capacity could be deployed, such as surveillance cameras, routines for engaging temporary staff, etc. According to what we can expect from an industrial frame, they looked upon both their own organization and the terminal’s external conditions as being stable (cf. Engdahl, 2003). Furthermore, their most obvious anxiety concerned group identity and whether dishonest insiders would be able to infiltrate their working groups when the use of temporary staff increased further.

This should be compared with respondents at the big-city terminal who expressed discouragement about their external conditions. They described an unreliable surrounding world that demanded personal initiatives from them. Despite the managers’ main responsibility, the workers underscored the fact that they had to contribute to the maintenance of security. The emphasis on hierarchic stability that belongs to an industrial frame was combined with a stress on individual responsibility.

This rather surprising view on terminal workers’ responsibility to act against perpetrators could be linked to the fact that this company had regional security officers who could do more to raise an awareness of security issues at a smaller number of terminals than the national officers in the other company. However, there are also figures that indicate that the big-city terminal is more exposed to theft, and a main reason why this shop-floor initiative was needed in the big-city terminal appears to be direct experiences of unreliable external conditions, rather than security officers informing workers about the problem, unions raising the question or management steering the workers indirectly (cf. Rose, 2000; Mythen and Walklate, 2006). Furthermore, even if the workers could describe actual interventions, the respondents did not think they were in control. Their wish for education on theft indicates that they experienced a lack of knowledge about how to act when they were exposed to perpetrators. Hence the terminal workers could be described as discouraged, rather than confident.

Table 2 describes the differences between industrial frames (Fisher, 1997) at the terminals in medium-sized cities and at the big-city terminal. Even if the anxiety regarding theft that respondents at the big-city terminal expressed with reference to unstable surroundings might not be expected within an industrial frame, we argue that the big-city frame should be described as industrial. After all, none of the big-city respondents claimed that they were exposed to authoritarian and arbitrary hierarchies that rendered them fatalistic vis-à-vis the surrounding world, that they belonged to a community of workers that limited insecurity and theft at work, or even that they as individuals had the capacity to handle rationally, all by themselves, external threats posed by, for example, professional thieves. They all viewed their position at work as defined by an industrial organization. However, it is an unconventional combination of different Grid and Group aspects that is expressed, which also implies that we are dealing with a security culture that has to be understood in a wider organizational context.
Explanations and further implications

As mentioned earlier, this study is based on qualitative interviews, which makes it difficult to measure any causal strength. However, we can point to some patterns in the way terminal workers framed this security problem, which help us understand why terminal workers expressed different industrial security cultures. These patterns give us important knowledge on how we should approach security cultures theoretically whenever we study such a phenomenon. They also help us understand how security cultures may guide employees in making sense of their own responsibility for security issues at work.

To begin with, we can say that our study illustrates that the work organization is an aspect that, despite differences in the terminals’ exposure to thefts, conditions the way in which security and theft are framed; the way that workers refer to well-defined and repetitive tasks is mirrored in how they describe the hierarchic organization of responsibility. However, we have also pointed to differences in how workers framed the terminals’ external conditions, which raises questions about the significance we ascribe to conditions at work. Our results indicate that we have to be aware of whether the internal organization is treated as the prime conditioner of how different security problems are framed. Employees in hierarchic or industrial bureaucracies should not automatically be expected to frame external conditions as stable just because they are working within hierarchic organizations (Douglas and Wildavsky, 1983). The internal organization of work is important, but the differences we found in this study illustrate how security cultures can contain frames of both stable hierarchies and external insecurity, a finding indicating that the security culture has to be understood within a wider organizational context.

We have already stressed that the big-city terminal was located in the centre of one of Sweden’s largest cities and was exposed to a large number of thefts and people coming and going, whereas the other two terminals were located on the outskirts of medium-sized cities. The statistics referred to above support the conclusion that the type of insecurity that the respondents at the big-city terminal associated with a demand on individual responsibility could partly be explained by the fact that their terminal was more easily accessed by a larger number of external and perhaps professional criminals. However, this recurring stress on external conditions also implies that an analysis of further external relations could

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Industrial frames of confident and discouraged terminal workers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group aspects</strong></td>
<td><strong>Grid aspects</strong></td>
</tr>
<tr>
<td>Industrial frame of confident terminal</td>
<td>Management has to take extensive</td>
</tr>
<tr>
<td>workers (terminals in medium-sized cities)</td>
<td>responsibility for the security.</td>
</tr>
<tr>
<td>The terminals have to be prevented from</td>
<td>Management can manage the problem of</td>
</tr>
<tr>
<td>potential insiders.</td>
<td>thefts/security within existing organization.</td>
</tr>
<tr>
<td>Theft/security is a limited problem to the</td>
<td></td>
</tr>
<tr>
<td>workers (the external world is stable).</td>
<td></td>
</tr>
<tr>
<td>Professional thieves and junkies make the</td>
<td>Management has to take extensive</td>
</tr>
<tr>
<td>terminals vulnerable to external conditions.</td>
<td>responsibility for the security.</td>
</tr>
<tr>
<td>External conditions demand individual</td>
<td>But the problem is becoming worse and</td>
</tr>
<tr>
<td>responsibility from the terminal workers.</td>
<td>the responsibility has to improve at the shop floor.</td>
</tr>
</tbody>
</table>

Table 2  Industrial frames of confident and discouraged terminal workers

<table>
<thead>
<tr>
<th>Industrial frame of confident terminal workers (terminals in medium-sized cities)</th>
<th>Industrial frame of discouraged terminal workers (the big-city terminal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group aspects</td>
<td>Grid aspects</td>
</tr>
<tr>
<td>The terminals have to be prevented from</td>
<td>Management has to take extensive</td>
</tr>
<tr>
<td>potential insiders.</td>
<td>responsibility for the security.</td>
</tr>
<tr>
<td>Theft/security is a limited problem to the</td>
<td>Management can manage the problem of</td>
</tr>
<tr>
<td>workers (the external world is stable).</td>
<td>thefts/security within existing organization.</td>
</tr>
<tr>
<td>Professional thieves and junkies make the</td>
<td></td>
</tr>
<tr>
<td>terminals vulnerable to external conditions.</td>
<td>Management has to take extensive</td>
</tr>
<tr>
<td>External conditions demand individual</td>
<td>responsibility for the security.</td>
</tr>
<tr>
<td>responsibility from the terminal workers.</td>
<td>But the problem is becoming worse and</td>
</tr>
<tr>
<td></td>
<td>the responsibility has to improve at the shop floor.</td>
</tr>
</tbody>
</table>
improve our understanding of how security cultures are shaped in different organizations. Each of these relations would probably demand comprehensive studies of their own. But, we cannot ignore the possibility that a security culture may depend on factors such as the relationship that a company has with other companies and other actors involved, for example, the police, the authorities and insurance companies.

**Hierarchies in a turbulent world – final remarks**

At the beginning of the paper we mentioned that insecurity at work in complex transport networks could be tackled by delegating responsibility from the top to self-governing individual employees (Rose, 2000; Mythen and Walklate, 2006). Still, most respondents in this study expressed an industrial frame of security. They described their responsibility as limited by industrial functions, clear routines and predefined procedures of work rather than shaped by managers propagating for self-conducted workers. The idea of flexible and self-governed workers trying to catch up with demands on new transports within a complex network would be an exaggerated description of these terminals (cf. Jones and Newburn, 2002). Instead of stressing uncertain and changing global demands, their joint industrial frame of routine-based and repetitive work implies that they saw themselves as workers within an industrialized transport network, designed to benefit from a calculated economy of scale (Lambert and Stock, 1993; Stefansson, 2004) and meet the needs from the consignee terminal for delivery within a certain time window (Ekwall, 2007).

We also have to recognize that workers at the big-city terminal seemed to work in an industrial hierarchy exposed to external conditions that, to a certain extent, reminds us of earlier descriptions of increasingly complex and ever-changing global transport networks, demanding that they did not just fulfil specified functions but also tried to secure freight transports, threatened by an insecure surrounding filled with professional criminality (cf. Castells, 1998). These respondents described intervention as a complicated or even discouraging necessity. Unlike respondents from the terminals in medium-sized cities, they wanted even more knowledge; they wished to be capable of handling the problem of theft themselves. We can therefore conclude that an industrial security culture does not exclude frames of daily security at work, in which initiatives from the shop floor and aspects of a self-governed worker are expected. However, we still have to investigate to what extent workers are likely to be given room for individual initiatives at the shop-floor level under such circumstances.

**References**


Security culture and transport network terminal activities

Daniel Ekwall¹, Bertil Rolandsson²

1: School of Engineering, University College of Borås, 501 90, Borås, Sweden
   E-mail: Daniel.Ekwall@hb.se, +46 33 435 59 72

2: School of Education and Behavioural Sciences, College of Borås, 501 90, Borås, Sweden
   E-mail: Bertil.Rolandsson@hb.se, +46 33 435 42 06

Abstract

Purpose – All freights within a transport network are to some extent scheduled. This predictability plays an important role in all potential crimes against the network. Several different supply chain security programs advocate for increased security awareness regarding potential security breaches. What are the organisational consequences in terms of security culture for terminal workers?

Design/methodology/approach – A semi-structured interview guide was designed, in order to facilitate both a theoretical focus and flexible conversations. 15 interviews were done altogether at three different goods/freight terminals, and each interview took approximately 30-45 minutes.

Findings – The management wants the terminal workers to perform their planned and scheduled operational tasks according to the written procedures. The security awareness idea advocates that, if needed, shall the employee perform security tasks instead of the planned operations. This means that the employees may be forced to choose between fulfilling their normal tasks or performing security duties. This duality in management signals restrained the development of security awareness.

Research limitations/implications – The research are limited by the difficulty in establishing clear and evident causal relationships between all the different factors that together compose the corporate security culture.

Practical implications – This paper shows that all management initiative affects the security culture in the transport network. In order to create the right security culture it is vital that all management initiative is understood from a user perspective and with a holistic approach.

Originality/value – Using theories from social sciences in logistics in order to fill the gap between the ideas from supply chain security programs and the real situation in the transport network.

Keywords: Security culture, Criminal activity, Transport network, Supply chain security programmes, Security awareness

Paper type: Research paper
Background

The increasing trend toward globalisation has led to an increase in logistic activity. The process of shipping goods around the world is long and complex (Schary et al., 2001), and yet the international trading system is dependent on the effective transport of these goods. Also, these transports have become more and more vulnerable. Christopher and Lee (2004) suggest that the increased vulnerability in supply chains is a result of the drive towards more efficiency, which in turn increases vulnerability from disruptions or disturbances. According to Svensson (2000), “Vulnerability is defined as the existence of random disturbance that lead to deviations in the supply chain of components and material from normal.” The outcome of such a disturbance should also have a negative effect on the companies involved (Svensson, 2000). This definition contains two difficulties; namely, the ideas of “random disturbance” and “deviation from normal.” Random disturbance indicates that the focal company does not control the change, while a deviation from normal suggests that there is such a thing as a normal or scheduled situation. The occurrence of a normal state is more probable in the transport network than in the flow of material. Thus the interactive sub-system of products and processes, using Juttner’s (et al., 2003) definition, is more flexible and thereby also possesses a larger tolerance towards deviation than the resources (facilities and cargo carriers) can manage. The transport network is therefore more vulnerable than the product flow, but the transport disturbance also affects the product flow.

This vulnerability can in many cases be described as “unwanted effects” in the supply chain caused either by internal or external forces that create disturbances larger than the supply chain is designed to handle. The disturbance can be unintentional or deliberate, legal or illegal. Today there is a significant problem with the theft of cargo worldwide. It is estimated that theft represents losses of at least US $ 10 billion per year in the United States and US $ 30 billion worldwide (Barth et al., 1998). These figures are extraordinarily conservative, because most cargo theft goes unreported and these figures reflect only the value of the items and nothing more (Barth et al., 1998). The theft of cargo value for the EU-area is estimated to be €8.2 billion each year. When allocated on all transports, this gives an average value of €6.72 per trip (EP, 2007). There are suggestions that the real figures for cargo theft in official reports are either grossly underestimated or overestimated (Gips, 2006). Gathering accurate numbers for cargo theft losses is difficult and in many cases impossible, due to limited reporting by the transportation industry and the lack of a national law enforcement system requiring reporting and tracking uniformity (ECMT, 2001).

In the CEN report (2006) Draft final report, different security measures are categorised into three different approaches: systematic, technological, and psychological. The systematic approach strives to establish action against threats and resilience as a response to incidents. The systematic approach also addresses different organisational aspects in supply chain security. The technological approach relates to the need for technological innovations to achieve a state-of-the-art technological advantage. The psychological approach aims to establish awareness among all personnel working within the transport network. The psychological approach can also be described as awareness or alertness within the transport chain. High awareness or alertness depends on the interaction and involvement of personnel in policy and business processes. Good awareness about problems with cargo theft must therefore be a part of the unwritten regulation of behaviour or a part of the company’s culture with regards to cargo theft problems. Several supply chain security programs such as C-TPAT (Customs-Trade Partnership Against Terrorism), CSI (Container Security Initiative), and AEO (Authorised Economic Operator) also emphasize the need for employee awareness in
order to increase the overall security level. Awareness together with the actual way things are done can be called the security culture (c.f. Fredericks, 1995).

Research question

The purpose of this paper is to analyse the security culture among terminal workers in a transport network. This is done against a background of increasing numbers of international supply chain security programmes that all more or less advocate security awareness among the employees as a cornerstone in security.

Security culture and transport network is a wicked problem

According to several authors (Rittel et al., 1973; Ackoff, 1974; Rosenhead, 1996), the term “wicked problem” is usable if the problem applies to issues or challenges that are not solvable by traditional linear and analytical methods. Wicked problems tend to be difficult to completely define and lack a clear end-point. A wicked problem is dependent on stakeholder judgments and interpretation. According to Rittel (1973), a wicked problem is unique because there are no solution principles that can be drawn from other wicked problems. Rosenhead (1996) suggested the following criterion for wicked problems:

1. Accommodate multiple alternative perspectives;
2. Function through group interaction and iteration;
3. Generate ownership through transparency;
4. Facilitate a representation of the solution space;
5. Focus on relationships between alternatives rather than continuous variables; and
6. Concentrate on possibility rather than probability.

The nature of a wicked problem is best described as being when a “…solution, after being implemented, will generate waves of consequences over an extended—virtually an unbounded—period of time. The next day’s consequences of the solution may yield utterly undesirable repercussions” (Rittel et al., 1973). This statement demonstrates that a wicked problem has multiple stakeholders; competing interests; multiple, fairly incompatible goals; and no universal solution (Peck, 2008). The security aspect within the transport network is therefore a wicked problem. To understand the problem, it is essential to understand the context, that is, both transport/logistics issues and corporate culture features. However, causality is very hard to establish, because everything is connected with everything else.

Frame of reference

The supply chain concept and transport networks

The framework of a supply chain normally has three major stages: supplier, manufacturer and customer. The need for coordination between all involved processes and companies to deliver value is basically what Supply Chain Management (SCM) aims to provide (Samaranayake, 2005). To obtain economy of scale in different production processes is it necessary to ship or transport product from site to site within the supply chain with the use of a logistics system.

A logistics system consists of links and nodes, where the nodes are geographically fixed points (such as factories and terminals) while the links are the elements connecting the nodes (the modes of conveyance or means of connecting the nodes). The links in the network can be
long or short. The physical flow of product through the supply chain is conducted by a transport network that is designed to use economy of scale when moving products from consignor to consignee in a supply chain, through nodes and links (Stefansson, 2004). The transport network affects cost and throughput time, and if used smartly it can increase the value of the product (Lambert et al., 1993).

All freights within a transport network are to some extent scheduled based on various reasons. One of the most common is the consignee terminal’s need for product delivery within a certain window of time. This makes the network predictable for all actors involved, including the potential perpetrator. This predictability plays an important role in all potential crimes within the network. The rigid scheduling in the transport network provides an excellent breeding ground for recurring crime opportunities (Ekwall, 2007). Even when recurring, the transport network will view a crime opportunity that is taken as an extraordinary event, something that is not a part of the usual pace in daily work. The terminal employees therefore need to be aware of such extraordinary events in order to minimize their consequences.

System of supply chains

Descriptions of supply chains are in general achieved with a system approach in logistics research. The description of the context and the boundaries of the supply chain are essential to understand the description of each supply chain. This is achieved as each supply chain is separated into several different sub-systems that together provide a wider understanding of the context and present different necessary boundaries. According to Är näs (2007), is it useful to separate logistics and transports from each other and instead emphasize the dialectic relationship between the terms or systems.

The logistics system is constituted of three structured elements/components: Products, Locations and Facilities. The transport system is constituted of three different structured elements/components: Vehicles/Vessels, Freight and Ways & Terminals. The dialectic relationship between logistics and transport is illustrated in figure 1.

![Figure 1: The dialectic relationship between logistics and transportation (Är näs, 2007).](image)
The joint positions (dialectic relationship) in figure 1 are the six different diagonal elements. Goods are represented by the terms Product and Freight, but from different perspectives. The infrastructure is also represented from two different perspectives as Location and Ways & Terminals. The relocation of goods using an infrastructure are represented by the processes of Forwarding and Movement (Arnäs, 2007). The dialectic relationship between logistics and transport provides an excellent description of the supply chain content products and infrastructure, but lacks the organizational element and also the wider environment that everything is acting within. By adding two additional systems to the logistics and transport is it possible to better elucidate the context and boundaries for a supply chain system.

According to Juttner (et al., 2003), a supply chain is an interactive system with four different levels. The first two levels correspond to the dialectic relationship between logistics and transport, while the other two levels represent the organizational structure and the wider environment. Each level includes various elements and content descriptions. These elements and descriptions are of a general nature and therefore not decisive; rather, they are more illustrative and explanatory. The main advantage of using four levels (or subsystems) to describe the supply chain system is that they automatically provide a contextual understanding and boundaries to the problem of antagonistic threats towards the logistics business. Further, to each level is attached a description of the major risk sources and the different risk management strategies normally used to handle (and hopefully minimize) the risk consequences attached to each level. A business generally considers the risk sources in the various levels differently. For example, a risk in level 2 is normally considered negative, while the same risk source may, in the perspective presented in level 3, represent a new business opportunity, which is normally considered good. Table 1 presents the system of supply chain risks.

<table>
<thead>
<tr>
<th>Level</th>
<th>Elements</th>
<th>Content Description</th>
<th>Risks</th>
<th>Risk Management Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Products and processes</td>
<td>Inventory and Information flows</td>
<td>Considered Bad: variance, inefficiency, lack of responsiveness, demand uncertainty</td>
<td>Substitution of information for inventory; better visibility, velocity and control</td>
</tr>
<tr>
<td>2</td>
<td>Assets and infrastructure dependencies</td>
<td>Fixed and mobile assets</td>
<td>Considered Bad: loss of link or nodes factors</td>
<td>Insurance and contingency/business continuity planning</td>
</tr>
<tr>
<td>3</td>
<td>Organisations and inter-organisational networks</td>
<td>Contractual and trading relationships, financial wellbeing</td>
<td>Considered Good and Bad: financial decisions/organisational failure</td>
<td>Contractually governed: partnering; dual sourcing; outsourcing</td>
</tr>
<tr>
<td>4</td>
<td>The wider environment</td>
<td>Economy, society and the forces of nature</td>
<td>Considered Good and Bad: geological, metrological and pathological forces of nature</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: System of supply chain with risk description and risk management strategies (based on Juttner et al., 2003 and Peck, 2008).
Most current logistics security programs have addressed different parts of level 2 while focusing on infrastructure risks, thereby achieving better security in the supply chain system. Programs such as AEO have glided a little closer to level 3 than other programs because it does criminal background checks (for customs crimes) on senior management of the certified company. This shall be compared with the corporate culture found in level 3 as it is a palpable part of all organisations.

Table 1 follows the logistics research tradition of not including people in the model or system. This may be a good approach in most logistics research but when the research question and purpose focus on the security culture, the research should be centred on human involvement. However, the supply chain system does not include cultural values such as security and team spirit. The reality in which the terminal worker acts is more complex and full of nuances in a way that logistics theories normally avoid. Terminal activities, security culture and team spirit can be described as functions that operate through group interaction and iteration, which is one of the criteria for wicked problems. Therefore, the inclusion of people and cultural values into logistics research aims to strengthen the knowledge base in logistics (Stock, 1997). An interdisciplinary exchange of views, ideas and theories is needed to develop logistics into an applied science (Klaus et al., 1993).

Security, risk management and crime prevention

Security, risk management and crime prevention are often considered similar and always work together (Manunta, 1999). This suggests that security and risk management are good, at least from an ethical point of view, because they reduce crime; thus more or better security or risk management should reduce problems caused by crime. The problem is that a crime is defined by law, according to the principle “no crime without a law”, while security or risk management has no philosophical attachment to the law. This means that people on both sides of the law can have better or worse security or risk management and that security and risk management are not necessarily for the prevention of crime. Unrestricted security for an individual or a group of individuals can jeopardise security for others by threatening them or transferring threats to them. This type of discussion can be heard from philosophers like Hobbes and Mills. Unbounded or unrestricted individual security could even threaten the authority of a state. Thus, a security problem may or may not be a legal problem. Security, as an idea, can be explained as having two parts: a protector or guardian and the threat it tries to protect the asset or object from. This threat can be from either side of the law. To obtain the right security it is vital to answer who is protecting what, from whom, in which situation, to what extent and to what consequence (Manunta, 1999).

Successful risk management needs to operate in a fairly predictable world or at least to be dependent on a large amount of trustworthy statistics. Because previous events or incidents are the basis of risk management, it cannot effectively deal with a self-inflicted alteration of the threat pattern. This means that, in crime prevention, statistical risk management is effective if the potential perpetrators are limited to the use of unsophisticated and indifferent methods that are based on opportunistic behaviour (Manunta, 2002). However, as potential perpetrators become more and more sophisticated and develop larger capability, the statistical predictability of risk will reduce dramatically. The antagonistic perpetrators study the victim to discover routines and regularities and with this knowledge they improve their skills (planning, technologies and tactics) to maximize their likelihood for success (Clutterbuck, 1987). The prevention of antagonistic threats by following current business trends makes the
system even more predictable. Military special forces and similar organizations have proven this time after time (Manunta, 2002). Thus a sophisticated potential perpetrator is better described as possible rather than probable. The more sophisticated or unique a certain threat is, the more plausible is it to describe the problem as wicked.

Transport and freight security

The security of freight transport was under-developed for a long time, but where terminal security has become better, theft incidents have increased in the links between terminals (Ekwall, 2006). This development is also valid from a supply chain perspective: while security in manufacturing facilities normally is both in focus and well-managed, the rest of the chain is without security (Purtell et al., 2006). The need or demand for security during transportation is to prevent unwanted negative disruption in the flow of goods. The general term for this prevention is transport security (EC, 2003), defined as the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems and workers against intentional unlawful acts (EU, 2003). Technological development in the range and sophistication of anti-theft devices and after-theft systems is increasing rapidly. Special attention has been given to systems that track the goods themselves throughout transport (ECMT 2001 - b); but applying different technological systems is only a part of transport security strategy (Tyska et al., 1983). The key issue is the successful coordination and cooperation of the actors involved in the transportation. At present this cooperation is not widely developed (ECMT 2001 - b). The lack of cooperation, together with other barriers in the business, is indicated by such things as underestimated risks from the haulers’ side; different standards in technologies; insurance companies that do not always give premium reductions; and technical standards that do not yet exist (ECMT 2001 - b). These barriers and lack of cooperation can be remedied by the use of common methods or standards in transport security (Tyska et al., 1983). Together with the police the operators’ associations can provide and disseminate advice and guidance to operators, especially regarding safe routes, parking areas with high security, precautions to take and appropriate equipment (ECMT 2001 - a).

Company security culture

According to Frederick (1995), the corporation is a complex and diverse conceptual construction. The legal entity (the corporation) has rights, privileges and liabilities distinct from those of its members. The corporation is first an economical construction designed to deliver profit for its shareholders. In order to achieve this, the corporation needs employees, equipment and capital, and the corporation should act within the local legislation. This complex construction contains both economical and sociological constraints which depend, to different degrees, on all stakeholders. Frederick (1995) argues that the anthropological conception of culture “as that complex whole” provides a potential synthesis. Frederick (1995) states:

Culture can indeed clarify the practices and policies of modern corporations, as well as the sometimes bizarre and distressing behaviour of those who work in corporations…capturing culture's meaning may unlock many doors within the corporate citadel.

According to Brinkman (1999), an understanding of the conception of corporate culture requires “a clarification of how the anthropologist's conception of culture relates to the
economic process overall”. This requires three elements that relate to the conception of corporate culture:

(1) The economic processes;
(2) The evolution of the economic and cultural form and structure; and
(3) The process of structural transformation.

Brinkman (1999) also maintains that culture is more than economics and material issues:

The mainstream economist focuses primarily on material culture and assumes the social and cultural, ceteris paribus, to be given. There are many reasons which are offered by mainstream economists as to why the social and cultural should remain outside the paradigmatic boundaries of analysis.

The real world description of products forwarded to every corner of the world through global networks clearly demonstrates that both social and cultural issues need to be within analytic boundaries instead of outside them. Consequently is it a good idea to describe the transport business as a comprehensive infrastructure requiring flexible and self-governing employees (Castells, 1996; 1998). Organisational complexity seems to be the rule. In several discussions about global and complex organisations such as transports, self-conducted staffs appear to be increasingly important for the coordination of security (Mythen et al., 2005; Kemshall, 2006). In accordance with discussions about the organisation of work and security, self-governing individuals could offer a way of coping with a broad spectrum of potential risks such as theft (Rose, 1999; Stokes, 2007). Managers, then, are tackling organisational insecurity caused by difficulties in controlling the organisational complexity by delegating responsibility from the top to the individual employee and assessing the outcome (Rose, 2000; Roberts, 2006).

Method

Data was collected through qualitative interviews at three different terminals. The use of qualitative interviews was motivated by the fact that the issue of the study is sensitive. Employees can be inclined to answer ordinary survey questions about thefts at their work in a politically correct way, which makes such data less reliable (Seidman, 1998). The problem of correctness does not vanish by using interviews, but it gives the opportunity to explain questions and to ask respondents to explain their answers. In addition, interviews always began with general and less sensitive background questions about the employee’s background and about the job. This helped the conversation to become more relaxed and allowed a sense of trust to be established between the interviewer and the respondent. This made it easier to go behind more formal descriptions of highlighted security problems (Kvale, 1997).

A semi-structured interview guide was designed to facilitate both a theoretical focus and flexible conversations. The guide was based on three main themes: the employee’s group identification at work, the organisational structure and aspects of the surrounding world such as temporary employees and unidentified visitors. The interviews began with less sensitive background questions, including employee age, years at work, and tasks typically performed. This helped to defuse the real issue. Fifteen interviews lasting approximately 30-45 minutes each were conducted at three different goods/freight terminals. It appeared that the theme of our study did not allow the conversation to be pushed longer. Furthermore, we interviewed employees at work; in many cases they had jobs waiting for them.
After the interviews had been transcribed, the transcriptions and what the employees had said during our conversations were analysed. Initially, theoretically anchored themes connecting different statements were used. These themes included “the surrounding world”, “group identity”, and “hierarchy”, and allowed us to also analyse different external and internal relations that the employees talked about. Codes indicating both whom and how employees connected thefts or other security issues with these themes were then used. The codes indicated both relations and contents (e.g. “insiders” or “prioritized/not prioritized question”). This made it easier to understand the meanings attributed to this issue and the similarities and differences that existed in the interpretative patterns at each terminal (Kelle, 1995). The latter also demanded a final and thorough confrontation with our theoretical point of departure: the underlying systematic and coherent conclusions about the security frames that were expressed at each terminal (Miles et al., 1994). The research procedure used in this paper can therefore be categorized as abductive (Dubois et al, 2002). The lack of previous research in this area makes the nature of this study explorative and therefore it focuses on the similarities rather than the differences within the interviews.

Empirical findings

Terminal description

The three different terminals involved in this research were all chosen by the researchers. The selection was made in accordance with the following criteria: The terminal should be owned by a major LSP company, situated close to the theft-endangered areas in Sweden according to official criminal statistics and willing to participate in this research. The chosen terminals belong to two different companies (A and BC). The terminals are located in three different cities; terminals B and C belonging to company BC were in mid-size cities while terminal A was located in a bigger city. The choice of interviewees was made at each terminal by the local site security officer (SSO). The guideline provided to each SSO was to choose blue-collar workers with a representative mixture of age, gender and length of employment at the company. During the interview, all normative discussion was held to a minimum. This was done to get the interviewees to state their true opinion and experience. For the same reason, all interviewees were guaranteed anonymity so they did not fear reprimands from their employers.

Crime risk around the terminals: official statistics

No complete and fully trustworthy statement about the problem of theft of goods in relationship with the European transport network exists. Still, it is reported that in some European countries up to one percent of cargo vehicles are stolen each year (ECMT, 2002). This is an indicator of the seriousness of criminal activities within the logistics business. Cargo theft, vehicle theft, theft of goods from vehicles and theft of entire vehicles loaded with goods have increased. The report “Organised theft of commercial vehicles and their loads in the European Union” (EP, 2007) states the cost for cargo theft in EU thusly: “The total loss of value can be estimated at more than €8.2 Billion each year. Of this amount about €450 million is not declared by the transport operators. If the loss value is related to the number of loaded trips, a value of about €6.72 per trip results”. As always, the numbers regarding antagonistic threats cannot be considered absolute but the numbers presented in this report have more credibility than normally is the case for this type of information. The report also states that 41% of all incidents occur during the driving phase of the transport while nearly 60% occur during a stop. The two most commonly used methods are threats towards the driver or tearing
up of the canvas of the load unit. In 15% of the incidents the truck is stolen with the goods and another 15% is hijacking and robbery.

The lack of reliable and comprehensive official criminal statistics with regards to crimes against the logistics business became obvious to the police authorities in south-western Sweden at the end of 2006. A project was launched to verify and compile all reported thefts and theft attempts but also to educate police officers in order to increase the quality of reports of future crimes. In January 2007 two unique report codes for crimes against the logistics business were created: 9803 (theft of a cargo carrier) and 9804 (theft of goods from a cargo carrier).

The official crime statistics for attacks against transports are 512 (2006) and 476 (2007) in the southwest of Sweden, where all three terminals are located. The attacks occurred mainly along major roads. Two of the terminals are situated at main road junctions and all of them are directly linked to one of the three major crime roads in south-western Sweden. According to Nilsson (2008), the number of unrecorded crimes is greater that those reported.

**Crime risk around the terminals: company risk ranking**

Neither of the two companies were willing to share their own statistics regarding thefts in the three terminals with the researchers because of business reasons, but they were willing to rank the terminals according to their perceived threat level (both companies have terminals in the same three cities) and cooperate without sharing statistics but by exchanging intelligence and information regarding threat levels. Both companies’ CSOs independently ranked the theft threat level for the terminals; the results were identical.

Official criminal statistics with both companies as injured parties give a different image of the risks to the terminals. Company BC is, according to the official statistics, more exposed for criminal attacks than company A. According to both CSOs, this difference can be explained because company BC has a policy to always report all suspected crimes while company A does not. Also, the official statistics with the companies as injured parties contain all types of crime against the company, not just theft; therefore these statistics give only a hint about the companies’ problems with criminality. The risk was considered highest for terminal A, followed by B and finally C. Table 1 shows the crime risk ranking for the terminals.

<table>
<thead>
<tr>
<th></th>
<th>Terminal A</th>
<th>Terminal B</th>
<th>Terminal C</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSO company A risk ranking</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>CSO company BC risk ranking</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Researcher risk ranking according to interview comments</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Reported crimes with the company as injured party 2006-2007</td>
<td>4 (company A) 130 (company BC)</td>
<td>26 (company A) 78 (company BC)</td>
<td>12 (company A) 57 (company BC)</td>
</tr>
<tr>
<td>Overall risk ranking</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

*Table 1: Risk ranking for involved terminals*
Security organisation in each company

The security organisation in both companies is set up in similar ways. In both companies they are considered secondary to the operational structure and instructions. In all three terminals there is an appointed Site Security Officer (SSO) with operational responsibility regarding security in the terminal area. The SSOs report to both the terminal manager and the security organisation. There is a difference in security organisation between the country’s Chief Security Officer (CSO) and the SSOs; there company A has an appointed regional security officer (responsible for a smaller number of terminals) with a preliminary coordinating function. Mutual in both cases is that the cost for security is part of the terminal manager’s budget and that the CSO holds a centralized staff function under the Managing Director. Company A has had a security organisation a few years more than company BC. This has led to a practical difference where company A has more and better implemented security guidelines and is more experienced when it comes to security issues. With this said, the security organisations in both companies are seen more as a necessary evil than as something that contributes to the bottom line (profit). In reality the security issues at each terminal are closely related to the SSO at each terminal while the central organisation only appears to do a security inspection or help the SSO to investigate difficult thefts.

Interviews

The interview guide used in all interviews was structured according to each individual’s experience of the work environment with regards to the security situation. This led to the use of three main themes in the interview guide: identification at work, the organisational structure and aspects of the surrounding world. The presentation of the interviews will follow this structure. All interviews were conducted in the native language of both the researchers and the interviewees, namely Swedish, and all quotes have been translated by the researchers.

Identification at work

In all interviews the work assignment was described as monotonous and repetitious tasks that were planned as parts of the general terminal process. For each individual this leads to insignificant possibilities to affect his or her own work assignment. Still, the general terminal function and need for personnel also entails positive effects for the employees. As one of the interviewees stated, “The assignments are mostly monotonous but with good working hours”. One drawback with monotonous and repetitious tasks was that staff turnover was described as either acceptable or high. In one terminal they described an extended use of seasonal workers in the form of students who worked for a shorter period. It was desirable for the number of personnel working at the same time at any of the terminals to be as low as possible, which led to an extended use of personnel from staffing companies.

All interviewees mentioned that the staff turnover entailed that they worked with relatively new people all the time. In some interviews this was considered as positive while in others this was seen as a negative effect. All interviewees identified themselves as blue–collar workers who were separate from the white collar staff.

Organisational structure

Both companies have adopted very similar hierarchical organisations that in both cases emphasise that there is a certain way to perform a certain task and this method should be
followed at all times. All responsibility within the companies and terminals comes from the top manager and is from there distributed throughout the hierarchy. The trust in top management to handle the companies or terminals is high. As one interviewee stated, “If there is a problem, I inform my boss and he solves the problem for me”. The interviews clearly proved that the entire general attitude towards uncertainty (regardless of type) is that it shall be reduced as far as possible. The basis of this idea is that equilibrium and stability exist in all logistics (Lambert 1998). In other words, everything can be controlled. The idea that everything can be controlled was the red thread throughout all interviews. Therefore it is possible to state that operational control is a vital part of the corporate culture.

Almost all interviewees provided one or more different narrative descriptions of self- or co-worker-experienced security incidents, mostly cargo thefts. As one interview described it, “I have captured a few guys red-handed with a computer theft. Other times investigations have led to thieves being captured who were colleagues, drivers or staffing personnel”. The uncertainty related to security incidents seems to threaten the cultural belief in operational control and organisational stability that was considered normal. The existence of thieves and other threats to operational control and organisational stability is a continuous generator of uncertainty and disbelief in management control functions, which generates waves of security cultural consequences over an extended period. Such a period can stretch to several years as some of the interviewees recalled security incidents years ago and repeated the experience to new colleagues.

The different organisational structures of the two companies could be identified in the interviews, where company A had tried to handle security-related uncertainty by creating a security organisation that was a little more locally based and the SSOs had a better understanding for what was expected of them and what they were allowed to do.

Aspects of the surrounding world

The threats or security risks that emerge from the world closely surrounding the terminal, which includes all insider-related issues, contributes to the feelings of security-related uncertainty presented in all interviews. As one interview described it, “The biggest threats come from the outside but that depends on the tip-offs from the inside the terminal/organisation.” Another said, “The thieves knew when and where the truckload of computers was here and how to steal it. They must have had information from inside to pull that one off.”

It was clear during the interviews that the mythical insider is, in actuality, far from a myth. Several of the interviewees knew of colleagues who been investigated and later sentenced for theft and thereby also discharged and blacklisted from the company. The presence of both eye-witness experience and mythical descriptions of insiders as one of the main security threats was in line with expectations based on previous studies and theoretical descriptions (Barth et al., 1998; Tryon et al., 1997; Muir, 1996; Beck, 2002; Speed, 2003). In all three terminals the discussion and description of insiders was similar; possibly the workers in terminal A had more eye-witness experience than the workers in the other two, but that might be because the interviewees in terminal A in general had been on the job longer. The effects on security culture from the insider problem can contribute to increasing distrust between personnel within the transport network. This is a negative impact, especially since general operational instructions are based on the idea that personnel trusts or at least checks that the previous operations were executed correctly.
The general descriptions of thieves contained everything from “pilfering” to “professional thieves”, with an emphasis on the latter. As one interview described it, “These guys that come here, they are professional, they are tremendously skilled and they are accordingly professional thieves. Thus they know when and how before they conduct the action.”

All interviews ended with how the interviewee ranked the security aspect of the company in relationship to other issues in their working environment. In almost all interviews other issues such as safety and general working conditions (temperature, ergonomics issues and working hours, etc.) ranked as more important than security. Those interviewees that had experienced security incidents were the most reluctant to write off the need for security.

Suggested security solutions from the interviewees were in most cases physical obstacles such as gates and fences together with surveillance cameras (CCTV). A few suggested better use of security procedures. The interviewees all believed that the hierarchical organisation will handle future security-related incidents and prevention so that they (the interviewees) can continue performing their work assignments as usual.

Discussion

In this study, all workers expressed a common belief in the higher hierarchy’s or organisation’s ability to design and implement procedures for all problems that may or may not occur at work. They described a legitimate hierarchy and a wish to keep the organisation and working groups honest and stable (Douglas et al., 1983; Engdahl, 2003). Rather than referring to themselves as autonomous individuals conducting complex jobs in an ever-changing transport network, they framed themselves as decent blue-collar workers at the bottom of the organisation. They complained about repetitive tasks, bad working conditions and poor communication with the top management, which delimited their own initiatives. However, it was also important that management followed established routines and procedures in the organisation (Mars, 1997). The interviewees all expressed the belief that terminal processes are designed, maintained and performed in accordance with the idea that equilibrium and stability exists in all logistics. There is no surprise that the presence of criminal actions in the logistics threatens the idea of stability and thereby also the strong belief that the hierarchical organisation will solve the problem. If the problem with security incidents increases (both occurrence and impact), the stress on the hierarchical organisation’s problem solving ability becomes greater. If the organisation does not prove its ability to handle security incidents, the terminal workers’ trust that the organisation can handle other issues may also be threatened and consequently the corporate culture will be altered.

Despite this contribution to the corporate culture, no respondent wanted a security organisation in which flexible individuals replaced hierarchical top-down control (Rose, 1999; Stern, 2006). Even though the big city terminal appeared to be exposed to less controllable circumstances, the workers claimed that it was mainly the management that had responsibility for cutting the risk of thefts at work. Most of them wanted to see more initiatives from the managers rather than from themselves, which underlines the importance they ascribe to a stable hierarchy. However, terminal A respondents described a need to intervene themselves. Based on our empirical material it cannot be determined whether they have been included in any decision-making dialogue. It can be said, however, that organised crime and the terminal’s location in the city centre meant that the workers felt that they had to take individual initiatives on the shop floor (Mars, 1984). Given that they knew about the security
policy and wanted more education about it, it may be said that they combined a wish for more initiatives from the management with features of self-governed workers who conduct themselves in accordance with knowledge, policies and rules of the company. However, the main reason why this shop floor initiative was needed appear to have been unpredictable external conditions rather than management steering the workers from a distance (Rose, 2000; Mythen et al., 2005). In line with Frederick’s (1995) argument that culture is a complex whole, this clearly demonstrates that if the corporate culture strongly emphasizes the hierarchic top-down control that conception will affect all processes and operations regardless of the demanded approach for special issues. This may lead to problems when security awareness depends on the interaction and involvement of personnel in policy and business processes but in normal logistics activities the involvement of personnel is held to a minimum.

Knowing the risk ranking for all three terminals makes it easy to draw the conclusion that a riskier surrounding affects security culture among terminal workers, but how this influence affects security efforts depends on several different factors. The right response and attitude from management may hinder a fatal disbelief in the organisation’s ability to prevent criminality. The response and attitude from top management all the way down to the terminal workers needs to result in the understanding of multiple alternative perspectives (top management’s, customer’s, terminals worker’s, etc.) and focus on relationships between alternative solutions instead of ad-hoc and stand-alone security features.

Conclusion

The international trading system is dependent on the effective transport of goods. These transports have become more and more vulnerable. Several supply-chain security programs such as C-TPAT, CSI, and AEO emphasize the need for employee awareness in order to increase the overall security level. Good awareness about problems with cargo theft must therefore be a part of the unwritten regulation of behaviour, or in other words, the company’s culture with regards to cargo theft problems. This awareness together with the actual way things are done can be called the security culture.

Risks can emerge from within both the organisation and the local environment. These risks can be described as uncertainties that need to be reduced as much as possible. This approach may be good for handling process failures but is less successful in reducing the problems with criminality within the logistics business. Management can, by interaction and involvement of personnel in policies and business process design, develop a more suitable security culture. This approach becomes more important if potential perpetrators become more and more sophisticated.

Normally, the different processes in terminals are designed to be simple and repeating, according to ideas from Lean production and similar logistics theories. The presence of security threats whose occurrence is unpredictable may force employees to choose between fulfilling their normal tasks or conducting security-related tasks, which also entails them to execute their normal tasks later and faster to reach the same level of productivity. This duality in management signals restrains the development of security awareness. The security culture depends on the organisational complexity in each terminal/company. To coordinate security in global and complex organisations, self-conducted staffs are increasingly important.

Reference:


Castells, M. (1998) *End of Millennium – The Information Age; Economy, Society, Culture vol. 1*, Malden, MA:


Impacts of the ISPS code on port activities: a case study on Swedish ports

Arsham Mazaheri* and Daniel Ekwall

School of Engineering
University College of Borås
501 90, Borås, Sweden
Fax: +46 33 435 40 08
E-mail: Arsham_Mazaheri@alum.sharif.ir
E-mail: Daniel.Ekwall@hb.se
*Corresponding author

Abstract: Following the terrorist attacks on the Twin Towers in the USA and the Limburg oil tanker in Yemen, the International Maritime Organization (IMO) agreed to develop new measures relating to the security of ships and port facilities. The impact of the International Ship and Port Facility Security (ISPS) code on port activities may have both positive and negative consequences on port services. This paper addresses the impact of the ISPS code from a total port perspective. This case study is based on an electronic questionnaire, which was developed with several qualitative pilot interviews with port security experts. The results are analysed in accordance with the structure of the ISPS code in order to establish the impact the ISPS code has on port activities. The results from this case study clearly indicate that an increasing security level in ports is the most important impact of the code. Better control of the port area, restriction of unauthorised access and a better working environment are examples of the effects that the implementation of the ISPS code entails on port and port activities. In addition to the ISPS’s advantages, there are some disadvantages, which can be summarised as higher operative expenses and a high implementation cost.

Keywords: ISPS code; port activities; supply chain vulnerability; port security.

Reference to this paper should be made as follows: Mazaheri, A. and Ekwall, D. (2009) 'Impacts of the ISPS code on port activities: a case study on Swedish ports', World Review of Intermodal Transportation Research, Vol. 2, No. 4, pp.326–342.

Biographical notes: Arsham Mazaheri is Research Scientist and PhD student at Helsinki University of Technology, Finland. He gained his Bachelor’s degree in Naval Architecture in 2005 from Sharif University of Technology, Iran and a Master’s degree in Logistics in 2008 from the University College of Borås, Sweden. He also has several years of work experience in shipbuilding industries. His current main research area is risk assessment in maritime safety and maritime transportation.

Daniel Ekwall is a PhD student at the School of Engineering at the University of Borås, Sweden. His research interests are supply chain risk management and antagonistic threats towards logistics products and systems.
1 Introduction

Following the terrorist attacks on the Twin Towers in the USA and the Limburg oil tanker in Yemen, the International Maritime Organization (IMO) agreed to develop new measures relating to the security of ships and port facilities. In December 2002, a new rule for security issues for ships and port facilities was defined by the IMO. Before adopting the International Ship and Port Facility Security (ISPS) code, the Safety of Life at Sea (SOLAS) had a chapter (Chapter XI) that contained special measures to enhance maritime safety. In December 2002, Chapter XI was renamed Chapter XI-1 and a new chapter (Chapter XI-2) was added on special measures to enhance maritime security. The ISPS code has been added as a supplement for this new chapter. Chapter XI-2 applies to passenger ships and cargo ships of 500 Gross Tonnage (GT) and upwards, including high-speed craft, mobile offshore drilling units and port facilities, which serve such ships engaged on international voyages. The ISPS code was entered into force on 1 July 2004 to reinforce maritime security and prevent similar terrorist acts against shipping.

The code contains two parts, of which the first part (A) is compulsory while the second part (B) is a guideline when implementing security provisions in Part A. Basically the ISPS code has been applied to safeguard maritime transportation security by ensuring that the security of ships and port facilities, onboard the ships and at the port/ship interfaces, will always be in place (IMO, 2003). The implementation of the ISPS code involves changes in both the physical design of the security in a port area and in general port activities. There are always concerns that a security rule goes far beyond what exactly is needed and then converts to an obstacle instead of being a good initiative (D’Addario, 2006).

The impact of the ISPS code on each ports security level is different depending on the local security need for each port. In ports with already high security, the proposed ISPS Security Level 1 may be lower than the current status. This leads to no impact from the ISPS code. On the other hand, in a port with very low security (even nonexistent), the ISPS code will dramatically change the security level, but the current security level may very well be sufficient for the local need. In this case, the implementation of the ISPS code is only seen as a compliance cost. With this said, it is plausible that the implementation will increase the security level of the port and also the security awareness of both employees and management.

This paper addresses the effects on ports depending on the implementation of the ISPS code in order to clarify any obstacles or good collateral benefits on port activities. The research question is, ‘What are the impacts on port activities of the implementation of the ISPS code in Swedish ports?’

The paper consists of several sections with all present vital aspects of the theoretical and practical background to the research question. It is also made of the methodology used during the research process and the empirical findings from the research. The paper ends with an analysis and conclusion of the research question.

2 Supply chain security

The 9/11 terrorist attack brought attention to the security in today’s trade. However, the reasons for better supply chain security are more than the risk for future terrorist attacks. According to Closs and McGarrell (2004), three factors can be outlined. First is the
globalisation of world trade, which depends on and is generated by the free flow of people, goods and information. Second is the increasing demand from businesses for efficient supply chain operations. Third is the increasing threat of terrorist attacks. This factor can be described as illegal and antagonistic threats, of which terrorists are one type. Therefore, supply chain security management can be defined as “the application of policies, procedures, and technology to protect supply chain assets from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain” (Closs and McGarrell, 2004).

The present supply chain security research outlines several changes in how security in a supply chain should be approached. First, supply chain security should incorporate not only theft prevention but also antiterrorism. Second, the focus is now on addressing global issues and not just local or national issues (Sweet, 2006). Third, when conducting contingency planning, the concept of crisis management is to be included to obtain better resilience. Last, security is no longer an internal corporate question but an issue for all actors within the entire supply chain (Closs and McGarrell, 2004). These four parts of supply chain security clearly advocate international regulated solutions like the ISPS code, but, depending on local variation in the need for security, the international supply chain security programme can result in either too high (costly) or too low (inadequate) security.

Lee and Whang (2003) suggest that methods and ideas from Total Quality Management can be used successfully to increase supply chain security. The main idea is the lesson from quality management that sample inspection is expensive and useless at the end of the production line. Just like in quality management, supply chain security becomes more effective and less expensive by implementing the right management approach and technology, and by reengineering operational processes. Lee and Whang state that security should be integrated throughout the entire supply chain to be successful at a reasonable price.

In recent decades, dependencies between companies and their suppliers have increased (Christopher et al., 2002). Some notions like Zero-Inventory and outsourcing have made companies more dependent on their suppliers and, as a result, more vulnerable (Waters, 2007). In addition, increasing globalisation and the complexity of supply chains lead the companies to greater exposure to risk from political and economic events (Harland et al., 2003). Any disruption to supplies or even consumers in a country can quickly affect an entire global supply chain and global trade (Khan and Burnes, 2007). An example of a disruption to supply is the sharp increase in world oil prices caused by the disruption of US oil production because of Hurricane Katrina (Khan and Burnes, 2007); for disruption to consumers, the recent downturn in the US housing market, which, coupled with high oil prices has, led to less consumption in the US markets and has spread fear of a pervasive downturn in global trade. These supply chain risk issues and sources differ from supply chain security features. Due to that, security is first of all intended to protect the flow of goods from illegal and hostile disruptions, while the supply chain risk theories cover a wider range of sources of disruptions such as like poor product quality and bad planning. With this said, the areas of supply chain risk and supply chain security are closely related and both address the supply chain’s vulnerabilities.

Mainly the supply chain’s vulnerabilities that come from the transportation side are classified as environmental risks. CLSCM (2003) defines environmental risks as “the risk associated with external and, from the company’s perspective, uncontrollable events”.

The environmental risks are more critical for companies to consider; nevertheless, they are uncontrollable events. The ISPS code addresses mainly the risks/threats from criminal activities such as theft, sabotage and terrorism. The nature of these threats is dynamic and is related to the surrounding environment, both geographical and political (Ekwall, 2008). Therefore, the ISPS code and its implementation need to be in control to prevent them from converting to a potential threat. This fact proves that “risk and security concerns are not a one-time issue but require a continuous risk management process” (Harrison and Hoek, 2005).

3 Port activities

The activities that a port normally has are highly dependent on the port’s specialty and size. For instance, the activities performed in a container port are different from the activities in an oil port. The same reasoning is valid from a size perspective. In general, most of the ports offer services like handling, storing, warehousing, value-adding services (stuffing, stripping, assembling, packaging, labelling, testing, consolidation, deconsolidation), intermodal transportation (by pipelines, trucks, trains, or even vessels for short sea distances), maritime services (pilots, tugboats, boatmen, vessel traffic control) and other services such as foodstuff preparation, power supply, ship repairing, recycling or even oil refining.

The ISPS code may have both positive and negative consequences on port services. This paper addresses the impact of the ISPS code in a total port perspective, which means that it does not distinguish one service from another but as combined parts of the port. This limits the scope of the research to only addressing the general aspect by analysing different activities/factors like staffing, lead time, service level, checking process, effectiveness and efficiency, with regard to the implementation of the ISPS code.

4 Methodology

4.1 Profile of participating ports

The participating ports varied both in size and in geographical location. They were mostly from the southern region of Sweden, where most of the Swedish ports are located. The smallest respondent port handled of 300 000 tonnes of cargo in 2006, and the biggest respondent port handled 40 000 000 tonnes of cargo in 2006 (Sveriges Hamnar, 2006). This paper defines ports as large or small in accordance with the following: a small port authority handles a few million tonnes, an average-sized authority handles between 10 and 20 million tonnes and larger ports handle over 20 million tonnes (Fourgeaud, 2000). The size difference between ports also implies differences in port activities, both in size, scope and performance. This difference should therefore be found in the impact of the ISPS code.

4.2 Data collection process

Electronic questionnaires were used to collect the primary data for this study. To prepare the questionnaire, the ISPS code and its related parts in SOLAS were analysed to elucidate those parts which could affect port and port activities. This analysis was
summarised into the first version of the questionnaire. The second step was three descriptive interviews with Swedish experts in maritime security. The reason for this was to verify both the relevance of the questionnaire and the general understanding of port security. These interviews entailed some changes to the questionnaire, including additional questions and possible answers. This process was conducted in order to increase the reliability of the collected data and also to increase the qualitative understanding of port security issues and their relation to port activities.

The electronic questionnaire was sent to persons who were in charge of the ISPS code in their ports, like Port Facility Security Officers (PFSO) or security managers. Before sending the questionnaires, they were informed via phone about the survey and its objectives and were also asked if they would participate in the study. Those who declined participation were not sent the questionnaire. The total number of Swedish ports with commercial traffic is 52 harbours (Sveriges Hamnar, 2006). Forty-two ports agreed to receive the questionnaire. All ports were given the same time to answer the questionnaire and if no answer was received by the researcher, they were contacted again. The participants were given all the time they needed to answer the questionnaire, which is a factor in a reliable data collection process. The Swedish port association provided help through with both the right contacts and a clear appeal to participate in this study. The ports that did not answer after the third inquiry were transferred to the nonparticipating ports category and deleted from the study’s sample population. All participants were promised that they would remain anonymous. The main reason for this was to increase the reliability of the data (Mishler, 1986).

The questionnaire had more than 40 single questions (and more than 60 nested questions). Because of the number of questions, the questionnaire was prepared in multiple-choice form to facilitate the participant’s answering of the questions. All the questions gave the option not to answer. This was done for security reasons. Attached to all questions was a comment section for those participants who wanted to add information.

4.3 Verification and validation of the results

Nineteen ports (45% of the involved ports, 37% of all commercial ports) answered the questionnaire. Among the answering ports were five of the ten biggest ports in Sweden; therefore the research result is reliable. In order to strengthen the credibility of this research, all ports were graded according to size, which was defined in terms of the cargo tonnage handled in 2006. (In this paper this is referred to as port value.) This increased the accuracy from 45% to 48%. The answers were analysed in two ways: one with consideration of the value of the ports and one without it. In case of significant differences, they were analysed to find the reasons.

5 Empirical findings

The general ISPS-related threats towards port activities in Sweden contain two different elements, namely cargo crimes and terrorism. The terrorist threats in Sweden are generally considered low or even nonexistent. This leads to the fact that the cargo crimes are the only pre-ISPS code-implementation security threat. Of the different types of cargo crimes, the most common is cargo theft. There are indications that the figures for cargo
Theft in official reports are either grossly underestimated or overestimated (Gips, 2006; Ekwall, 2007). The total loss of value for the EU area is estimated to be €8.2 billion each year, which, allocated to all transports, gives an average value of €6.72 per trip (EP, 2007). Gathering accurate numbers for cargo theft losses is difficult and, in many cases, impossible, due to limited reporting by the transport industry and the lack of a national law enforcement system requiring reporting and tracking uniformity (ECMT, 2001).

The lack of reliable and comprehensive official criminal statistics with regard to crimes against the logistics business became obvious for the police authority in south-western Sweden at the end of 2006. A project was launched to verify and compile all reported thefts and theft attempts and also to educate police officers in order to increase the quality of future-reported crimes. The official crime statistics regarding attacks against transports is 512 (2006) and 476 (2007) in South-western of Sweden (Swedish Police Authority, 2008). The attacks occurred mainly along major roads. According to Nilsson (2008), the number of unrecorded crimes is greater than the reported one. This leads to the fact that the official statistics only partly illuminates the problems with cargo thefts. The specific cargo theft statistics for ports (south-western Sweden) are included in the above-stated official statistics. The general conclusion from these statistics is that cargo theft is a lesser problem in Sweden than in other countries.

Consequently, the hostile and illegal threats against ports in Sweden must therefore be considered to be low. Thus many ports may have a lower need for security that what the ISPS code recommends. The result is that the implementation of the ISPS code is probably considered as a compliance issue and thereby mostly a cost-increasing feature instead of a security-increasing programme, irrespective of any collateral benefits.

5.1 Implementation difficulties

The participating ports were asked about their level of compliance with the ISPS code before its implementation and the amount of effort needed to meet the requirements. According to findings, the compliance level was dependent on the port’s size. The result, without port value, shows that 38% of the participating ports were already 30%–50% in compliance with the code’s requirements. When the ports’ values were considered, about 52% of the respondent ports were 50%–70% in compliance before its implementation.

It also shows that the smaller ports had a lower level of ISPS compliance before its implementation. Therefore, their investment and overall effort to achieve ISPS compliance was larger than that of the bigger ports. This shall be considered together with the fact that smaller ports handle fewer ships and a lesser amount of cargo. Therefore, the smaller ports’ ISPS cost/unit will be higher than that of the larger ports. As a result, the smaller ports will suffer a relatively higher cost structure for implementing the ISPS code. This is similar to the result that the United Nations Conference on Trade and Development (UNCTAD, 2007) mentioned in its report about the ISPS code’s financial impacts and level of compliance:

“The unit cost analysis revealed the presence of important cost differentials between respondent ports, especially between larger and smaller ports. In other words, relative costs appear to be substantially higher for smaller respondent ports.... results suggest that the ISPS code-related financial impact is more pronounced in the case of smaller ports.”
This result was been replicated when UNCTAD used different reference points like tonne of cargo throughput, TEU throughput, ISPS port facility or even ship calls.

Furthermore, the findings that implementation cost for the ISPS code was relative to the port size was also demonstrated, as an important majority of participating ports (71%) have not reached the economical break-even point. This number would change if the port sizes were taken into account. In this situation, a minority of the participating ports (43%) would reach the break-even point. This shows that larger ports have a shorter Return-of-Investment (ROI) time than smaller ports. This could be understood as either larger ports invested less than what the smaller ports did (regarding their annual revenue), which is supported by UNCTAD (2007) results, or larger ports had more cargo turnover, which contributed to the shorter ROI time.

The main initial investment cost for implementing the ISPS code’s expected security equipment like fences, gates and security systems was, in some cases, close to ten million SEK. The entire costs were, in all participating ports, placed on the local port’s own cost with no possibility for subsidisation from the Swedish port authority. According to McNaught (2005), the collateral benefit of lower cost for thefts is a vindication for the implementation cost. But this effect will be insufficient for smaller ports. As one of the interviewees answered regarding the question about reaching the break-even point:

“Will never do, since we are only a … [small] port.”

This quote strengthens the conclusion that the smaller ports regard the ISPS code as a compliance issue and thereby also as primarily a cost-increasing regulation.

5.2 Cost payer

According to the ISPS code, the security level of a ship and port facility should be at the same standardised level if the ship will be allowed to moor in a port. If the security level of either the ship or port facility is higher than the other, then the party with the lower level of security should increase its level so that both ship and port facility reach the same security level. To increase the security level in a ship imposes extra procedures rather than equipment; will the security cost issue be of lesser importance for the ship than for the port? According to the results from the questionnaire, there is no predefined model for the distribution of costs depending on the ISPS code. Therefore, is the direct ISPS-related cost negotiable between all potential ships and ports? This leads to the cost structure being one of the weaker points in the implementation of the ISPS code. This consequence is also indicated by Stevenson (2005), who points out that the cost unit has not been clarified.

5.3 Time window

The overwhelming majority of the respondent ports (89%) had problems with the time window for implementation of the ISPS code. Most probably this was caused by the fact that the time gap between adopting the code and its implementation was not sufficient. Some ports were also disappointed that the Swedish port authority did not provide the ports with clear directives and information about the code implementation. This could also be caused by the short time frame from the proposal to when the code became valid. The short time frame did not allow the port authority to become fully aware of the code requirements and what needed to be done in order to achieve the ISPS code in time.
5.4 Human rights

Several authors (Griffett, 2005; Stevenson, 2005; McNaught, 2005) point out the effects that the ISPS code has on seafarers’ lives and that it may restrict human rights and limit access to the ship. Stevenson (2005) hints that most of the problems for seafarers are caused by some ports that are following the words of the ISPS and not the spirit. It seems the Swedish ports are more eager to follow the ISPS code’s spirit rather than its words, since most of the respondent ports (88%) have proclaimed that they did not have any problem about seafarers’ lives and human rights violations. Moreover, nearly 80% of the participating ports believed that issuing an international identity document like the Seafarers Identity Document (SID) or Maritime Security Identification Card (MSIC) can address any possible problems related to seafarers. It should be stated that all of the ports that reported some problems about this matter declared that an international identity document could solve it.

Furthermore, it is possible that some ports require extra payment for seafarers’ shore leave or ship access. Even though all the respondent ports declared that they do not require extra payment, it is possible that some of them included it in their tariffs, since 31% of the ports have increased their service prices (Figure 1). Albeit this is not a major issue in Swedish ports, it is possible that it is in other countries. This depends on their interpretation of the ISPS code in relation to human rights.

5.5 Different interpretation

McNaught (2005) and Stevenson (2005) believe that different interpretations of the code in different countries is one of the ISPS code’s weaknesses. For instance, according to one of the interviewed security experts, the border of the area protected by the code in Denmark was defined just by yellow lines, while in Sweden it was defined by fences. The European Union (EU) member states have tried to address these problems by allowing security professionals to interpret the ISPS code. The same security professionals were also designated to inspect port facilities in EU. However, this problem still remains in other sections of the world. The results show that the Swedish ports are not really involved with this problem. Seventy-one percent of participating ports declared that they have not been involved in such problems.

5.6 Poorly trained officers

The problem with poorly trained security officers may have existed prior to the ISPS code, but it became obvious with the implementation of the ISPS code. According to Part A of the ISPS code, Sections 13 and 18, the security officers must be trained to be able to handle all the duties that would be delegated to them. Therefore, logically, the problem with poorly trained security officers should disappear with the implementation of the ISPS code. The reality is different as some companies are not enthusiastic about taking the training of the security officers seriously. Consequently, having poorly trained security officers may cause some problems, especially in relation to the ISPS code and its implementation. According to the participating ports, 77% have had no problem with poorly trained security officers, while just 8% of them had numerous untrained officers. It seems not to be an important issue in Swedish ports, even though an interviewee was disappointed about the untrained Ship Security Officers (SSO) who visited their port:
“I have most experience with untrained SSOs. Some do not know much about the rules. Depends largely on the attitude of the Flag State and also of the company…”

On the other hand, the ports were asked about any possible arguments or problems that they had with ship or cargo owners relating to the ISPS code. The results show (as before) that it is probably not a major issue in Sweden. With this said, most of the few cases of untrained security officers happened at the beginning of the code implementation. This problem has clearly declined as everybody is getting more and more familiar with the ISPS code.

5.7 Working on Security Level 3

One possible scenario that could happen, while the ISPS code is ruled in ports, is when the security level is set on the highest level. ISPS Security Level 3 shall only be used if an imminent attack is happening or expected. According to Security Level 3, 100% of the cargo shall be checked, while for Level 2 the volume checked is 20% and for Level 1 only 5%. This difference between the three security levels clearly demonstrates that the higher security levels are more time consuming and costly than the lower ones. It is possible that some ports would prefer to close down all port activities than to operate under ISPS Security Level 3. In terms of supply chain vulnerability, could this be interpreted as the intruders having succeeded in disrupting the port’s activities and thereby influencing global business? Therefore, the ports were asked about general port activities under ISPS Security Level 3. The results were truly favourable; 59% of the participating ports would still work at ISPS Security Level 3 and 9% of them have answered that it will depend on the cause of the alert.

Nonetheless, the result was not decisive if the alternative answer ‘prefer not to answer this question’ was interpreted as ‘No’ instead. The outcome would almost shift. Seventy-two percent of the ports would not work at Security Level 3, while 4% of them have associated it with the cause of the alert. This is not a situation that would be desirable for governments. The unwillingness to answer the question may refer to the fact that ISPS Code Level 3 is, for Swedish ports, very far from their idea of needed security. Several of the interviewees expressed this opinion. Whether the ports will or will not be operating under ISPS Security Level 3 needs to be seen when ISPS Security Level 3 is demanded by the authorities for the first time in Sweden, which still has not occurred.

5.8 Serving time

The relationship between the ISPS code implementation and serving time for ships was addressed in the questionnaire. It was found that since all the security checks and customs formalities must be performed before the ship reaches its port of call, the loading and unloading time has not noticeably changed. Therefore, it could be understood that the serving time has almost remained unchanged. This leads to the conclusion that applying the ISPS code has increased the security and not entailed changes in the serving time. The implementation of the ISPS code has therefore led to some advantages being gained without losing anything. The sealing of the port area for exterior people has resulted in an improved work environment. This leads to higher effectiveness for cranes, lift trucks and
other equipment at the port facilities due to the operators having fewer uncertain elements in their working environment. This was expressly commented on by several of the participating ports. This could indicate one of the main advantages of the ISPS code.

5.9 Part B of the code and related concerns

The interpretation of ISPS Code Part B may lead to problems due to the existence of discordance. Following the adoption of the code, the USA declared that compliance with Part B would be mandatory for US flag ships and all foreign flag ships visiting the USA. This shall be compared with EU Regulation No. 725/2004, which made some sections in part B of the ISPS code mandatory for EU member states (The European Parliament and the Council of the European Union, 2004). Furthermore, ISPS code Part A was stipulated as mandatory for domestic Class A passenger ships. The discordance in the rest of the countries is based mainly on the fact that they have not made such a decision for their territories. This leads to the possibility that discordance regarding ISPS Code Part B induces unwanted business trouble. The participating ports stated that EU Regulation No. 725/2004 did not have any undesirable impacts on global trade and business. Results show that 70% of the respondent ports believe that it has had no impact, while just 30% of them have accepted that it might cause some problems. It should be mentioned that 45% of the respondent ports preferred to not answer this question. The mixed feelings regarding considering Part B of the ISPS code as mandatory or not was clearly illuminated by one of the participants as follows:

“I don’t agree that part B is [mandatory] only for US and European countries. It is in the SOLAS that is global for ships over 500 tonnes. That’s the reason to set the regulation under SOLAS to make it mandatory for all ships.”

This statement also sheds some light on the discordance regarding ISPS code Part B: the SOLAS calls attention to ship size, which the EU regulation does not. With this said, the results presented in this paper regarding this issue are incomplete due to the geographical limitation that is used in this study. Therefore, the conclusion is limited to discordance over regarding ISPS code Part B as mandatory or not. Further conclusions regarding discordance effects on general business relations are impossible to state.

5.10 Indirect impacts

In the questionnaire, the ports were asked about the indirect impacts of the ISPS code on their activities in addition to the security level. The factors which were asked about had been defined according to supply chain elements like lead time, administration cost, service level and customer satisfaction to find how the ISPS code has affected the supply chain’s vulnerabilities as a means to mitigate supply chain risks (Figure 1).

A majority of the participating ports (80%) noted an increase in security level, which is the main goal of the ISPS code. Therefore, it is possible to conclude that the implementation was mainly successful in fulfilling its main purpose. With this said, the increased security level in Swedish ports could lead to fewer problems with cargo crimes, like smuggling and theft, and also better control in port areas (Wengelin, 2006). The general threat level in Sweden for terrorist attacks was described by one of the interviewees:

“We do not think our port is of great interest for terrorists…”
Figure 1  Indirect impacts of the ISPS code besides the impact on security level

This statement was fully expected from a general point of view with regard to terrorist threats in Sweden, as these types of threats are considered as a very unlikely threat or something that happens abroad.

In comparison, other factors like documentation, the checking process and administration costs were reported to have increased by a majority of the participating ports; whereas factors like lead time, effectiveness, service level and occurrence of damage have been less affected by the implementation of the ISPS code. The participating ports had a mixed attitude towards factors such as profit, manning, customer satisfaction, service price and competitiveness. This could be caused by the fact that the effects of the ISPS code have not been linked to these factors by the ports.

To clearly analyse the impact of the ISPS code on port activities as summarised in a number of factors, it is useful to divide the results presented in Figure 1 into two different groups depending on whether the study indicates an increase or decrease in relation to the efficiency of the ports. Group 1 constitutes positive factors while group 2 represents the negative factors. This analysis is presented in Tables 1 and 2.

The results presented in Tables 1 and 2 are further combined into an overall analysis on the impact on port activities of the implementation of the ISPS code. The conclusion regarding port efficiency alteration dependent on the ISPS code is presented in Figure 2. All numbers in Figures 1 and 2 as well as in Tables 1 and 2 refer to the number of ports and not to port value.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Positive factors in port efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group 1</strong></td>
<td><strong>No effect (%)</strong></td>
</tr>
<tr>
<td>Profit</td>
<td>63</td>
</tr>
<tr>
<td>Service level</td>
<td>80</td>
</tr>
<tr>
<td>Effectiveness</td>
<td>81</td>
</tr>
<tr>
<td>Security level</td>
<td>20</td>
</tr>
<tr>
<td>Competitiveness</td>
<td>67</td>
</tr>
<tr>
<td>Customer satisfaction</td>
<td>53</td>
</tr>
</tbody>
</table>
Table 2  Negative factors in port efficiency

<table>
<thead>
<tr>
<th>Group 2</th>
<th>No effect (%)</th>
<th>Increase (%)</th>
<th>Decrease (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manning</td>
<td>60</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>Lead time</td>
<td>86</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>Documentation</td>
<td>13</td>
<td>88</td>
<td>0</td>
</tr>
<tr>
<td>Checking process</td>
<td>13</td>
<td>87</td>
<td>0</td>
</tr>
<tr>
<td>Occurrence of damage</td>
<td>71</td>
<td>0</td>
<td>29</td>
</tr>
<tr>
<td>Administration cost</td>
<td>25</td>
<td>75</td>
<td>0</td>
</tr>
<tr>
<td>Service price</td>
<td>69</td>
<td>31</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 2  Impact of the ISPS code on the ports’ efficiency

According to the results presented in Figure 2, the conclusion of a majority of the participating ports is that the ISPS code has had no significant effect on their activities. The number of ports that state a decrease in port efficiency is bigger than the number of ports that express an increase in their efficiency.

This general statement about port efficiency was compared with the outcome of the direct question in the questionnaire regarding the overall change in port efficiency. The result is presented in Table 3.

Table 3  Distinction between believed and stated port efficiency effects from the ISPS code

<table>
<thead>
<tr>
<th>Source</th>
<th>No effect (%)</th>
<th>Increase (%)</th>
<th>Decrease (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2</td>
<td>54</td>
<td>18</td>
<td>28</td>
</tr>
<tr>
<td>Direct questions</td>
<td>47</td>
<td>53</td>
<td>0</td>
</tr>
</tbody>
</table>

The participating ports generally believe that the implementation of the ISPS code has resulted in higher port efficiency. This result provides an interesting view of the impact of the ISPS code. The general belief is that the implementation has involved both efficiency improvements and drawbacks, but all in all the improvements have exceeded
by far the drawbacks. One reason for this difference between experienced increase in port efficiency and the changes in different factors that altogether affect the efficiency may depend on the viewpoint or position of the representative(s) who answered the questionnaire.

Altogether, does this remarkable result express the fact that port efficiency is being affected noticeably by factors other than those mentioned in the questionnaire? These additional factors, according to UNCTAD’s (2007) report, could be additional security personnel, access control, screening measures, the introduction of port worker badges, better internal organisation and better planning of container yards and ships.

5.11 Port satisfaction

The ports’ level of satisfaction in applying the ISPS code can be another factor to evaluate the code’s success. If the port size is taken into account, the level of satisfaction will not change significantly. The satisfaction level of the largest population of the participating ports (32%) is set to more than 90% satisfaction with port value. This level would decrease to between 70%–90% without considering the port value. The port satisfaction levels, according to the participating ports, are presented in Figure 3. This strengthens the credibility of the conclusion that the ISPS code works better for larger ports than for smaller ones.

Figure 3 The ports’ satisfaction level

The overall level of satisfaction with the ISPS code implementation can be summarised in Figure 4. ‘High level of satisfaction’ represents those ports that were more than 50% satisfied with the implementation of the ISPS code. ‘Low level of satisfaction’ represents those ports that were less than 50% satisfied with applying the code.
As can be seen, the overwhelming majority of the respondent ports (91%) are satisfied with the implementation of the ISPS code in their port areas, which is another point for the ISPS code. The unsatisfied ports explained their view on the ISPS code implementation with:

“We have no choice [!]”

“Who can stay outside and still operate on international business?”

Both of the statements above relate more to the fact that implementing the ISPS code is mandatory, and not that the different ports can directly get new business opportunities. However, the relationship between the satisfaction level from implementing the ISPS code and improving the percentage of port activities due to the code is not palpable. The comparison between the ports’ answers about improving the percentages of their activities and the satisfaction level indicates a weak causal relation between satisfaction level and the improvement level depending on the ISPS code. This leads to the interesting idea that the improvement in their port activities is not really an important factor in satisfying the port administration. According to the results, nearly 90% of the participating ports have reported a low level (lower than 50%) or even no improvement in their activities relating to the ISPS code. With this said, nearly 50% of the ports preferred to not answer this question, which reduced the possibility of drawing far-reaching conclusions. For instance, factors like security level could be a more powerful parameter in satisfying the port administration in parts of the world other than Sweden. Therefore, we can conclude that the satisfaction with the ISPS code is more related to local port external factors than to the ISPS code itself.

The question is, why did half of the respondent ports prefer to not answer this question? There is a possibility that they lacked a detailed and exact view about the improvement in their ports, and consequently they preferred to not answer the question. This conclusion is supported by a comment from one of the participating ports:

“Hard to give firm answer, think in the long run the port activities have improved.”

Based on the statement above, it could be expected to have more improvement in port activities by time lapse.
6 Conclusions

The ISPS code’s main mission is to address security issues in maritime transportation. Although the initial reason for the ISPS code was terrorism, other security-related issues like smuggling, theft and piracy can be addressed by its implementation. Increasing the security level in ports is the most important impact of the code. Better control of the port area, restriction of unauthorised access and a better working environment are examples of effects that the implementation of the ISPS code has on ports and port activities.

In addition to the ISPS’s advantages, there are some disadvantages, which should not overshadow its benefits, but should be considered to make its impacts as effectual as possible. The disadvantages can be summarised as higher operative expenses and high implementation cost. This research supports the findings of other authors (Stevenson, 2005; McNaught, 2005), namely that one of the main problems about the code’s implementation is the lack of a predefined model for the distribution of costs.

Generally, the hostile and illegal threats against ports in Sweden are considered to be low. Thus the ports may have a lower need for security than what the ISPS code recommends. The result is that the implementation of the ISPS code is probably considered as a compliance issue and thereby mostly a cost-increasing feature instead of a security-increasing programme, irrespective of any collateral benefits. This paper shows that the smaller ports in Sweden had a lower level of ISPS compliance before its implementation. Therefore, their investment and overall effort to achieve ISPS compliance was larger than that of the bigger ports.

In addition, some factors like more documentation, more administration, extra checking and extra staffing make it difficult to judge the code’s integrity. It really depends on the price that someone wants to pay for security. Moreover, it seems that the ISPS code is better designed for large ports than smaller ones. This conclusion is visible in the lower satisfaction level among smaller ports. With this said, the overwhelming majority of the respondent ports (91%) are satisfied with the implementation of the ISPS code on their port areas.

The conclusion from this research can be presented in terms of the advantages and disadvantages, depending on the implementation of the ISPS code, as follows:

1 General advantages of the ISPS code:
   • better safety and security and lower risk
   • better control on the port’s area, flow of goods and personnel
   • better documentation (having a unit standard for documents)
   • better working environment.

2 General disadvantages of the ISPS code:
   • work slows down progress
   • more paperwork
   • more costs
   • more administrative work.
The ISPS code affects a large part of the different port activities. The research clearly indicates this as 17% of the participating ports believing that the ISPS code did not have any disadvantages, while only 7% mentioned that it had no advantages. A majority of the participating ports (80%) noted an increase in security level, which is the main goal of the ISPS code. Consequently, factors like security level could be a more powerful parameter in satisfying the port administration in parts of the world other than Sweden. Therefore, we can conclude that the satisfaction with the ISPS code is more related to local port external factors than to the ISPS code itself.

Overall, the ISPS code is like a train that is moving while railroad tracks are being laid. There were many issues that needed more consideration before its execution, such as human rights matters and models for the distribution of costs.

Acknowledgements

The authors would like to thank all the port administrators and port security officers of Swedish ports who contributed to this study by answering the questionnaires.

The financial support of this paper comes from both the University College of Borås and the Swedish Governmental Agency for Innovation Systems (VINNOVA). The authors would like to thank both organisations for their trust and support.

References

Centre for Logistics and Supply Chain Management (CLSCM) (2003) Understanding Supply Chain Risk: A Self-Assessment Workbook, Cranfield School of Management, Centre for Logistics and Supply Chain Management.


IMO (2002) Safety of Life at Sea, SOLAS.


