

Thesis for the Degree of Licentiate of Engineering

Report 67

Antagonistic gateways in the transport network in a supply chain perspective

Daniel Ekwall

Division of Logistics and Transportation
Department of Technology Management and Economics
Chalmers University of Technology
Göteborg, Sweden 2007

School of Engineering
University College of Borås
Borås, Sweden 2007

Antagonistic gateways in the transport network in a supply chain perspective

© Daniel Ekwall, 2007

ISSN 1652-8026

Report/Department of Logistics and Transportation, Chalmers University of Technology: 67

Division of Logistics and Transportation
Department of Technology Management and Economics
Chalmers University of Technology
SE-412 96 Göteborg, Sweden

ISSN 0280-381X

Skrifter från Högskolan i Borås: 2

School of Engineering
University College of Borås
SE-501 90 Borås, Sweden

Antagonistic gateways in the transport network in a supply chain perspective

Abstract

The World Trade Centre terror attack in 2001 changed the world and with it the conditions for logistics world-wide. The aftermath to 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 by either 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 also either legal or illegal. This thesis addresses the problem of deliberately caused (antagonistic) and illegal action against legal logistics.

There are basically two types of illegal and antagonistic threats to logistics, theft/sabotage and smuggling. The theft/sabotage problem is directly aimed toward the logistics activities, while smuggling abuses the logistics system for illegal purposes. The reasons behind these problems can vary from case to case as well as the different countermeasures to prevent these problems to occur. This thesis addresses only this problem in the transport network and sees the network as a part of a supply chain. In each part of the transport network there is a certain risk associated with the goods. All these risks together form the total risk for the transport or the transport network.

The research in this thesis follows the tradition in logistics to use a system approach to treat the research questions. The system approach also implies a top-down perspective on the system, or in this case the two systems, but the research questions address only the cross-over points between the two systems. The main method for this thesis is deductive. Both primary and secondary data are used to support the deductive and theoretical conclusions. This thesis is also based on the result of five different studies within this topic.

The perpetrators' decision process is the key issue to understanding the usage of antagonistic gateways in the transport network. The preferred risk management approach is therefore contextual instead of statistic, when preventing the usage of antagonistic gateways. In other words, the countermeasures need to be based on an understanding of this decision process, the antagonistic dynamics of potential perpetrators. This understanding is to a large part also an understanding of the context in which the perpetrators act. The difference in perpetrator context is easily described with the difference between regular cargo thieves and ideology-driven perpetrators or terrorists. The thieves are after the monetary value that the cargo represents, therefore they prefer to steal high-value, untraceable and highly demanded products. The ideological perpetrator or terrorist wishes to make a statement with the attack, therefore he will sabotage products, which will give the statement attention and (if possible) understanding for it. If a potential terrorist desires to finance an upcoming terrorist attack by means of cargo theft, the perpetrator will act as a regular cargo thief. This difference in perpetrator context is vital for applying the right type of countermeasures in the transport network. Security against these types of antagonistic threats in the transport network aims to alter the contextual perception of the network and thereby reduce the problem of antagonistic gateways.

Keywords: Supply Chain Management, Transport Network, Risk Management, Crime Prevention, Cargo Crimes

Preface

This licentiate thesis has been written at the School of Engineering at the University College 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. I would therefore like to thank you all.

The financial support of this thesis comes from both the University College 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 presented in this thesis depend on the cooperation from all involved companies and organizations, which have shared information, discussed theories and the reality with me. Without their experience and knowledge the result would not have been the same.

First, I am full of gratitude towards my supervisor, Professor Håkan Torstensson. Without his support, advice and trust in me, this thesis would never been completed. His cooperation and correction has really made the difference in this research. Secondly, I would like to thank Mr. Timothy Tinney, M.Sc., at the University College of Borås for his help with the English language and for all good input to the research result. During the research process several other colleagues at the University College's section for quality-driven logistics have provided support and contributed to the outcome. Thank you all. I would also like to thank the helpful personnel at the library & learning resources department and the rest of the employees at the University College of Borås.

A special thanks to professors, colleagues and other personnel at the Division of Logistics and Transportation at Chalmers University of Technology for all help during the research process.

My thanks to all my friends, who, despite my never-ending talking about the research, continued to be my friends. A special warm acknowledgement to my family for the belief you have had in me.

Last, but by no means least, all thanks for all support I have received from my wife Lovisa. Without your understanding and encouragement, I never would have been able to finish this thesis. I love you.

Borås, December 2006
Daniel Ekwall

List of appended papers

PAPER A:

Cargo theft from supply chains: Crime displacement in logistics

Daniel Ekwall

Earlier version presented at ASIS, Security Solutions for the Future Copenhagen
17-20 April 2005

Submitted to:

Supply Chain Management: An International Journal

PAPER B:

Differences in Black and White Logistics System Design

Daniel Ekwall

Submitted to:

International Journal of Physical Distribution & Logistics Management

PAPER C:

The role of temporary storage in a supply chain perspective

Daniel Ekwall

Submitted to:

The International Journal of Logistics Management

Table of content

List of figures	IX
List of tables	IX
1. Introduction	1
1.1. <i>Background</i>	1
1.1.1. Cargo theft	2
1.1.2. Smuggling of goods	2
1.1.3. The European situation	3
1.1.4. Current situation in Sweden	6
1.2. <i>Purpose</i>	7
1.2.1. Research questions	8
1.3. <i>Delimitations</i>	8
1.4. <i>Outline of the thesis</i>	9
2. Frame of reference	10
2.1. <i>The supply chain concepts and microeconomics</i>	10
2.1.1. Principles of microeconomics	11
2.2. <i>Risk and uncertainty in the supply chain</i>	11
2.3. <i>Supply chain security</i>	13
2.4. <i>Security and risk management</i>	14
2.5. <i>Logistics and transportation</i>	17
2.5.1. Transportation and freight security	20
2.6. <i>Criminological theories used in this thesis</i>	22
2.6.1. The two different outlooks on mankind in criminology	22
2.6.2. The elements of crime	23
2.6.3. Opportunity to crime	23
2.6.4. Routine activity perspective	24
2.6.5. Situation crime prevention	24
2.6.6. Crime displacement	25
2.6.7. The professional vs. the opportunistic perpetrators	26
2.6.8. Internal or external perpetrator	27
2.6.9. Security, risk management and crime prevention	28
2.7. <i>The deductive framework for this thesis</i>	30
2.7.1. The supply chain perspective	30
2.7.2. The transport network perspective	31
3. Methodological framework	33
3.1. <i>Research procedure</i>	33
3.2. <i>System approach</i>	33
3.3. <i>Research process</i>	34
3.4. <i>Data sources and their reliability</i>	36
3.5. <i>Interviews</i>	37
3.6. <i>Verification and validation of results</i>	38
4. Results	39

4.1.	<i>Link between appended papers and the two studies</i>	39
4.2.	<i>Paper A: Cargo theft from supply chains: Crime displacement in logistics</i>	41
4.3.	<i>Paper B: Differences in Black and White Logistics Systems Design</i>	42
4.4.	<i>Study 3: Crimes against commercial traffic (Dillén et al, 2006)</i>	42
4.5.	<i>Paper C: The role of temporary storage from a supply chain perspective</i>	43
4.6.	<i>Study 5: Statements about antagonistic gateways</i>	44
5.	Conclusions	48
5.1.	<i>Theoretical conclusions</i>	48
5.2.	<i>Generalisation</i>	50
6.	Further research	52
7.	References	53
	Appendix 1 – List of organizations involved during the research process	60
	Appendix 2 – Questionnaire for the statements about antagonistic gateways in the transport network	62

List of figures

<i>Figure 1: The produce/acquire matrix and legality of the business</i>	1
<i>Figure 2: System-theoretical outline of this thesis</i>	8
<i>Figure 3: Theoretical background for this thesis</i>	10
<i>Figure 4: Sources of supply chain risks (Christopher et al, 2004)</i>	12
<i>Figure 5: Cause/consequence matrix for cargo incidents</i>	15
<i>Figure 6: Levels of logistics (Wandel et al, 1995)</i>	17
<i>Figure 7: The four flows of logistics</i>	18
<i>Figure 8: Transport network with gateways (Lumsden, 2006)</i>	18
<i>Figure 9: Transport network with temporary stops</i>	19
<i>Figure 10: Risks and uncertainty in the transport network</i>	19
<i>Figure 11: Security in the transport network</i>	21
<i>Figure 12: Perpetrator's characteristics matrix</i>	27
<i>Figure 13: The supply chain perspective with gateways between logistics flows</i>	30
<i>Figure 14: The transport network perspective with antagonistic gateways between systems</i>	31
<i>Figure 15: The transportation security in relationship with antagonistic gateways</i>	32
<i>Figure 16: The relationship between the five studies conducted in this thesis</i>	35
<i>Figure 17: Antagonistic gateways in the transport network in a supply chain perspective</i>	49

List of tables

<i>Table 1: Value and number of incidents (road transports) reported to TAPA during the period September 1999 to December 2000(Winterburn 2005)</i>	4
<i>Table 2: Value and country (road transport) reported to TAPA during the period September 1999 to December 2000(Winterburn 2005)</i>	4
<i>Table 3: Year by summary of incidents and value (Winterburn 2005)</i>	4
<i>Table 4: Presentation of procedures and year of thefts (Winterburn 2005)</i>	5
<i>Table 5: Presentation of product type (Winterburn 2005)</i>	5
<i>Table 6: Reported thefts against transportation through the E18 corridor 2003-2005 (NCO 2006)</i>	6
<i>Table 7: Table of differences between holistic and reductionist approaches (White 1995)</i>	16
<i>Table 8: Classification of the five studies</i>	35
<i>Table 9: Relationship between the three papers, the two other studies and the research questions in this thesis</i>	39
<i>Table 10: Statements, answers and addressed issues in study 5</i>	46

1. Introduction

This thesis examines the subject of antagonistic threats to supply chain performance. These threats can basically be divided into two categories, abuse of the system or theft from it. The thesis addresses these threats in a supply chain perspective. Chapter 1 introduces the research questions, their motivation, the scope and the delimitations of the study.

1.1. Background

The foundation in all trade is the ability to move or transport the product from the source to the customer and still make money, a profit from trade. The foundation in all businesses can be described as the two fundamental major problems, to find or create demand and how to supply it. The supply side can further be described as the question of how to produce or how to acquire parts of or the complete product. 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 to acquire goods to meet the customer's demand. Figure 1 illustrates the produce/acquire dilemma from a legal point of view.

Acquire	Purchase of wholesale goods	Theft of wanted products
Produce	Manufacture	Manufacture of counterfeited products / non-intellectual rights
	Legal	Illegal

Figure 1: The produce/acquire matrix and legality of the business

If a company decides to produce or acquire can be seen as a risk assessment strategy based on a cost-benefit-analysis. It is normally agreed, that a larger business risk will require a larger expected profit, for someone to do business. The business risk is commonly stated as the likelihood for a negative incident combined with the economical impact of that incident. These incidents can be either unintentional or deliberate. The deliberately caused incidents can also be called fulfilled antagonistic threats. Not all antagonistic threats are illegal but some are.

The World Trade Centre terror attack in 2001 changed the world and with it the conditions for logistics world-wide. The aftermath to 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 caused and also either legal or illegal. This thesis addresses the problem of deliberate caused and illegal action against legal logistics.

There are basically two types of illegal and antagonistic threats to logistics, theft/sabotage and smuggling. The theft/sabotage problem is directly aimed towards the logistics activities while the smuggling abuses the logistics system for illegal purposes. The reasons behind these problems can vary from case to case as well as the different countermeasures to prevent these problems to occur.

1.1.1. Cargo theft

The risk for theft of goods during transportation has been around since the first transportation occurred. The theft of goods is a well-known phenomenon some of the most famous cargo thieves are Robin Hood (from literature) and Sir Francis Drake (English privateer during the late 16th century). No country, no commodity and no shipper are exempt from the acts of cargo theft (EU, 2003). It has been shown that cargo theft is a grave threat to modern trade. 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.

Today there is a significant problem with the theft of cargo worldwide. It is estimated that theft represents losses of at least US \$ 10 billions per year in the United States and US \$ 30 billion worldwide (Barth et al., 1998). These figures are calculated extraordinarily conservative, due to that most cargo theft goes unreported and these figures reflect only the value of the items and nothing more (Barth et al., 1998). There are predications that the real figures for the cargo theft is in official report 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 - b). Even the insurance business do have problems to separate frauds from real thefts and even if they had accurate numbers they would not want to share it with the public due to trade secrets and ability to compete within their business. 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 (EU, 2003).

1.1.2. Smuggling of goods

The illegal transportation of goods, smuggling, is a newer problem (but still very old) than the cargo theft. That depends only on the fact that it needs laws and regulations that restrict transportation of the goods. The primary target of the smuggled 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). The buyer of these illegal products is everywhere (Johns et al., 2003). Smuggling of products does not necessary mean that the product is illegal everywhere. What is legal in one country can be illegal in another one. This leads to that the actors in

smuggling can be legal companies that try to access a, for them, prohibited market. An example of this was Western companies that smuggled products into the former communist countries during the cold war era.

A linked problem with smuggling is the manufacturing of products without intellectual rights, the production of counterfeited goods. All that had been produced can be so again, by someone else. In terms of contraband it means simply that everything can be a counterfeited product (IACC, 2005). In order to bring the counterfeited products from the production site to the end user it has to cross several national boundaries (in general) 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 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 is placed where the risk for detection is low in combined with the normal white business problem of where to produce its products, as different types of costs and quality aspects. The illegal products are then distributed by using the trade routes and port activities in the same way as legal logistics do (Naylor 2004). The pollution of illegal products in the legal transport network is agreed to be a serious problem. The most common countermeasure taken against smuggling is inspection of cargo carrier when it crosses a national border. These inspection, do by there pure existence, creates disturbance in the transport network, even if no illegal product is discovered. By preventing illegal products to enter the transport network will this type of disturbance be avoided at the same time as smuggling will be prevented.

1.1.3. The European situation

There exists no complete and fully trustworthy statement about the problem in Europe about both thefts of goods and smuggling in relationship with the European transport network. The knowledge about theft problems is generally considered better than about smuggling. This is due to the fact that it is more difficult to hide a theft than a smuggling attempt. In some of the European countries up to one percent of cargo vehicles become stolen each year (ECMT, 2002). This is an indicator of 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. In Europe, the theft of cargo carrying vehicles alone has 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% were hi-jacks. The types of 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 theft of goods during transport is also a growing problem, 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 representative for their members, who transport more desirable goods than in general) both the location and the mode of procedure are distinguishing for the problem. The relationship between the stolen value and procedure is strong. Hi-jacks represent 25% of the incidents, while they represent 46% of the value.

<i>Procedure</i>	<i>Value in US\$ (millions)</i>	<i>Number of incidents</i>	<i>Value/incident</i>
Hi-jacks	15.8	38	410 526
Terminals	8	28	285 714
On the way	6.7	58	115 517
In parking spaces	3.7	21	176 190
Jump ups	0.1	5	20 000
Total	33.9	150	

Table 1: Value and number of incidents (road transports), reported to TAPA during the period September 1999 to December 2000 (Winterburn 2005)

If these numbers are presented related to the country where the incident occurred, the following view of the problem is obtained.

<i>Country</i>	<i>Value in US\$ (millions)</i>	<i>Number of incidents</i>
France	13.4	34
Great Britain	6.9	43
Italy	2.6	8
Netherlands	2.6	13
Belgium	2.4	6
Germany	2.1	11
Sweden	0.7	3
Turkey	0.6	1
Spain	0.5	7
Other countries	2.1	24
Total	33.9	150

Table 2: Value of loss per country (road transport), reported to TAPA during the period September 1999 to December 2000 (Winterburn 2005)

The two tables above present a picture of theft incidents in Europe, targeting companies that trade with high value products. To the value or direct cost in the above table indirect costs or losses, like customs duty and taxes shall be added.

More recent numbers from TAPA EMEA present a better picture of the theft problem in Europe.

<i>Year</i>	<i>Value in US\$ (millions)</i>	<i>Number of incidents</i>
2000	30.5	131
2001	39.3	118
2002	69.2	234
2003	72.8	334
2004	59.4	344

Table 3: Yearly summary of incidents and value of losses (Winterburn 2005)

A presentation of these incidents according to modus will give the following result.

	2001	2002	2003	2004
Terminal	36%	29%	22%	17%
Parking	1%	0%	6%	14%
Hi-jacks	8%	11%	13%	13%
Lost during transit	20%	21%	14%	13%
Stolen lorry	4%	4%	11%	12%
Jump up	23%	24%	23%	12%
Failed theft attempt	0%	0%	1%	7%
Fraud	2%	1%	5%	6%
Airport	1%	3%	1%	3%
Secure parking	5%	6%	4%	2%
Illegal	0%	0%	0%	0.3%
Total	118	234	334	344

Table 4: Distribution of theft methods over four years (Winterburn 2005)

A view of the most wanted products gives the following image of what the thieves aim for.

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

Table 5: Share of product types over four years (Winterburn 2005)

The numbers presented in table 3, 4 and 5 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 4 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 during 2004 is that the problem has moved from terminals and out to the links between terminals, in this case road transport in general.

1.1.4. Current situation in Sweden

During a workshop in May 2006 for the project SecureFlow'05, representatives from the Swedish police and logistics companies discussed the trends and the present situation regarding criminality against transportation in Sweden. A survey of reported thefts (crime classification numbers 0876, 0883 and 0821) through the E18 corridor for the years 2003-2005 is presented in table 1.

Reported theft				
County	2003	2004	2005	Sum
Stockholm	546	412	176	1134
Västmanland	33	27	25	85
Örebro	30	32	8	70
Värmland	49	30	25	104
Sum	658	501	234	

Table 6: Reported thefts in transport through the E18 corridor 2003-2005 (NCO 2006)

The expert group made the following analysis of the trends of transport-related theft throughout the E18 corridor:

- The willingness to report theft has decreased, which can depend on that the police can be difficult to reach and that the internal cost to make a report is greater than the gain from doing so. The hidden statistics in transport-related theft has become larger.
- The companies in the transport business have become more professional with regard to security. The actual number of thefts has decreased.
- The freight customers have increased their demands on security. The actual number of thefts has decreased.

The expert group considered the statistics from the E18 corridor valid for the trend in Sweden during the same time period. The proportions of the theft problem indicate that the uncertainty in the statistics has increased, mainly because of decreasing willingness to report incidents. Despite the increasing hidden statistics, the expert group concluded that the actual number of incidents has decreased. The general development indicates that the theft attacks against the transport network have moved out on the roads or at least outside the terminal walls. Theft from parked vehicles has increased, even inside terminal areas. Two main reasons for this development are the companies' key handling and that they park loaded vehicles in the terminal area over the weekend. The problem with hi-jacking of lorries carrying freight has not reached Sweden so far. One reason for this is that it is still too easy to obtain the goods the "normal way".

In Sweden the E18 corridor is not the great problem. The problem area can be described as the area reachable within a 2-2.5 hours' drive from Göteborg. In reality this means a triangle from the northwest of Skåne to Jönköping (sometimes as far as Linköping) and back to Göteborg. There are cases that describe incidents north of Göteborg up to southern Värmland. The general trend in Sweden is falling, except in Jönköping. The capital area surrounding

Stockholm represents a problem area on its own without substantial contact with the problem triangle.

Attacks against parked lorries (estimated numbers 2005)

- Göteborg 9
- Jönköping 97
- Kronoberg 40-50
- Helsingborg 40 (first quarter of 2006)

These parking spaces can be seen a market for goods exchange between different drivers and even an alternative fuelling station, because sometimes drivers steal diesel fuel from other lorries. The most difficult part of investigation for this type of crime is the difficulty to establish the actual place of crime. Normally the theft is only first discovered at the consignee's terminal or in the next reloading point in the transport network.

The transport business itself has three different problem areas that are believed to be the weak links in a security and anti-theft perspective.

- Company culture; Terminal workers and drivers still see it as an employment benefit to bring home "damaged goods".
- The transport network is not designed for today's way of shopping. Today electronics and computers are transported, yesterday screws and nuts were.
- Secure parking spaces.

The thieves prefer certain products (according to the expert group):

- Car accessories
- White goods
- Electronics like computers, laptops, digital cameras, MP3-players etc.
- Fashion or branding clothes and shoes (may be commissioned jobs)
- Alcoholic products and tobacco

A large volume in a certain theft indicates that it is probably a commissioned job. The thefts are seasonal and the stolen goods sometimes end up in other countries.

1.2. Purpose

The aim of this thesis is to enlighten the cross-over points or antagonistic gateways between the legal and the illegal logistics systems from a supply chain perspective. This research is intended to combine theories from criminology with theories from logistics and supply chain management. This new theoretical framework is then strengthened with statistics, interviews and case studies about cross-over points between the two logistics systems.

1.2.1. Research questions

The overall aim for both legal and illegal logistics system is to provide the right product at the right place and time, and to do this cost-effectively. The two systems are not strictly parallel but more of a simultaneous occurrence; therefore a single transport of cargo can contain products from the both systems. To prevent this mixture of goods in systems is to govern the two systems to become more parallel. This is achieved at the different gateways or cross-over points where the products may or may not change system.

- RQ 1 What are the characteristics of the antagonistic gateways between legal and illegal logistics systems?
- RQ 2 How can these gateways be prevented?
- RQ 3 What are the effects on transport network design of the existence of antagonistic gateways?

1.3. Delimitations

This research is impregnated by a system-theoretical approach, which emphasizes a holistic view instead of the characteristics of different parts. The scope of this thesis is that there are two different systems used as descriptive tools. They are both logistics systems with the overall purpose to provide the right product at the right time and place to the right customer. The difference between these systems is the legality of them, where one of them is legal and the other one is illegal. Each product is a part of either the legal or the illegal logistics system. In this thesis a product that is completely legal is a part of the legal logistics system, otherwise it is a part of the illegal one. In reality the boundary between the legal and the illegal system is more of a greyscale than a distinct limit. The most important in a system is its boundaries and the context in which it is presented (Wilson, 1990). In this thesis the context is logistics and supply chain management and the boundaries are the legality of the goods. The main focus of this thesis is the cross-over point between the two systems, or when a certain amount of goods is transferred from one system to the other.

The research is based on a deductive method that uses theories from both logistics and criminology to form a new framework to study these cross-over points between the two logistics systems that are used in this thesis. The new framework is then validated with official statistical from several different independent sources together with interviews.

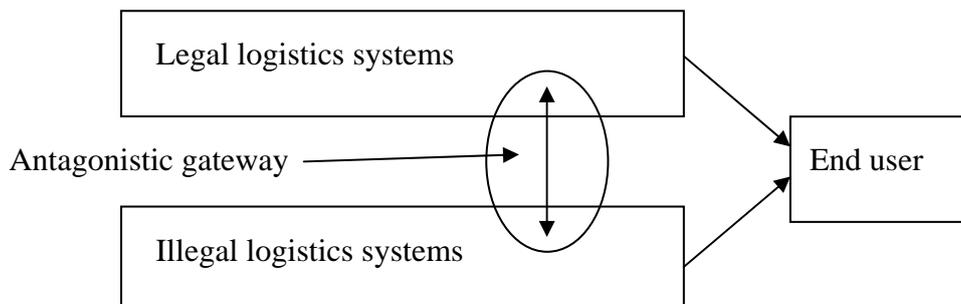


Figure 2: System-theoretical outline of this thesis

The research in this thesis addresses only the gateway or cross-over point between the two logistics system and how these can be categorized and prevented.

There exist several types of crime that can be linked to the transportation business. This thesis does not address the problems from a juridical viewpoint. Therefore several different types of crime can lead to the usage of a cross-over point between legal and illegal logistics systems. The commonly most known crime types for usage of the antagonistic gateway are crimes like robbery, theft, burglary, pilfering and smuggling of goods or humans. There also exist a number of linked crimes that could occur together with the usage of an antagonistic gateway, namely fraud, corruption, tax evasion, terrorism, sabotage, money laundry and different types of violence crime (Naylor, 2004, Burnett, 2002, Findlay, 1999, Napoleoni, 2004, Larmour et al., 2001, Clutterbuck, 1987). With this said, this thesis acknowledges the differences with regard to definition and modus for these different crimes. This thesis does not clarify the differences according to the criminal code, i.e. different methods, modus etc. that distinguish one crime type from another, when it comes to the antagonistic gateway between the two logistics system.

1.4. Outline of the thesis

The outline of this thesis is presented in this chapter and shall be seen as a guide to the reader.

Chapter 1 provides a background reflection and emphasizes the aim and practical relevance of this thesis. This is achieved with the presentation of research questions and delimitations based on the scope and purpose of the thesis.

Chapter 2 provides the frame of reference for the thesis. This is the theoretical foundation for the research and, as the method for this thesis is deductive, this chapter contributes strongly to the credibility of this research.

Chapter 3 presents the scientific approach and its application in the research. At the end of this chapter validation and credibility are discussed.

Chapter 4 presents the results that this thesis brings forward. The chapter includes a summary of the five studies that the thesis is based on. The five studies are presented in the form of three papers, one report and one statement survey, conducted to verify the theoretical conclusions presented in chapter 2. This chapter also provides a discussion of how these studies are linked to each other and to the thesis.

Chapter 5 provides the concluding discussion of this thesis.

Chapter 6 is a brief exposition of future research subjects in the field.

2. Frame of reference

This chapter introduces the framework that is the backbone of this thesis. The framework aims to combine the two scientific fields of logistics and criminology in order to reduce the risk for usage of antagonistic gateways in the transport network. The perspective is from a logistics view and the aim is to reduce certain risks within the supply chain. This is achieved by applying criminology theories into logistics and not the other way around. The theoretical background to this thesis is illustrated in figure 3.

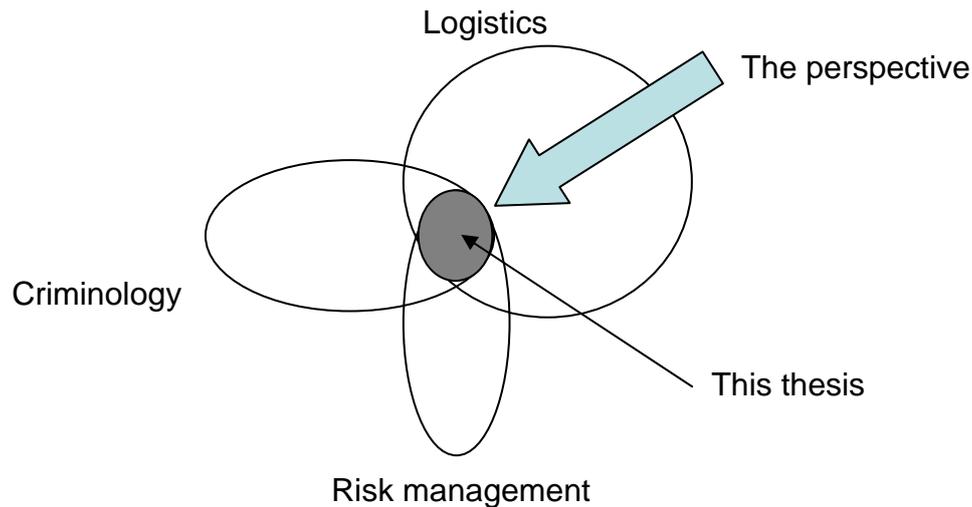


Figure 3: Theoretical background for this thesis

2.1. The supply chain concepts and microeconomics

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 that co-operate to fulfil the scope of logistics is called the supply chain. The supply chain is therefore a network of autonomous or semiautonomous 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. The framework of supply chain normally has three major components, namely supplier, manufacturer and customer. With this said, all supply chains end at the end user and begin with the preparation of the raw material. The current economic trends have instead of emphasising the need for vertical integration (e.g. economies of scale) argued for the need for specialization. This trend has forced and is forcing 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 basically what Supply Chain Management (SCM) aims to solve (Samaranayake, 2005). To demonstrate the importance of SCM Christopher already in 1992 stated that in the future supply chains will compete instead of single companies (Christopher, 1992).

The managing of the total or smaller parts of the supply chain 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 flexibility to respond quicker to actual customer demand, all while keeping the costs down (Samaranayake, 2005).

2.1.1. Principles of micro economics

The principles of micro economics 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 by inducing general principles from the scientific field of micro-economics. Mankiw (1997) uses 10 principles to explain why certain decisions are economically rational or not. 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 on that the above-stated principles of micro-economics are valid and important to comprehend to be able to understand why people decide to break a law in order to make money. The first four principles (1-4) concern human behaviour, principles 5 and 6 state that the marketplace is the place for economic transactions, and the last four principles (7-10) explain the government's involvement in business.

The first principle implies that people have a choice in all trade. It can be simplified as follows: "Is the expected reward (profit) larger than the expected risk (cost)?" This statement also contains large portions of the third principle. The fifth principle illuminates the driving force behind trade with no linkage to the law. In all these principles, the law can be seen as either a reward or a disadvantage, depending on which side of the law the particular actor is on. These principles provide a general understanding of mankind, trade and expected outcome from actions. The ten principles shall be seen as an invisible red thread through this thesis.

2.2. Risk and uncertainty in the supply chain

Historically, security and vulnerability within the supply chain were largely neglected until the terrorist attack on the World Trade Centre. The subjects of supply chain 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. Christopher and Lee suggest that the increased vulnerability in supply chains is a result of the drive towards more efficiency, which also in turn increases vulnerability from disruptions or disturbances (Christopher et al, 2004). 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).

Risk and uncertainty are often seen as synonymous (Helliard et al, 2001). But 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.

The concept of risk combines probability and consequence for a certain event (Wang et al, 2000). 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.

According to Christopher and Peck (2004), 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. 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). 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). Figure 4 illustrates the relationship and interdependency of the five sources of supply chain risk.

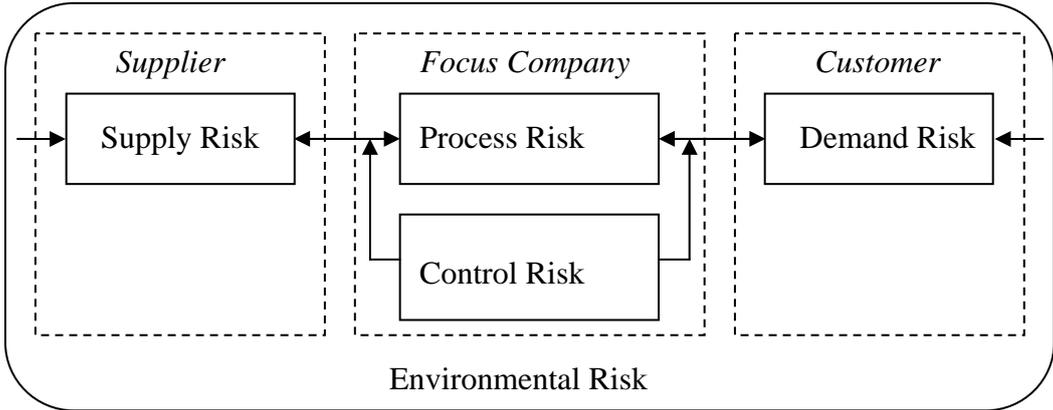


Figure 4: Sources of supply chain risks (Christopher et al, 2004)

This means that the demand and supply risk addresses disturbance in physical distribution, through in- and outbound logistics activity. Risk consequences or the disturbance can be either 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 can also 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 risks and from which direction they come in a supply chain. The term sources do not refer to the actual cause of the incident. The term risk refers to a probability for an event and a negative economical impact of that event. The risk is the expected value of an issue or event. With this said, the discussion of risks in the supply chain is a good way to describe negative effects in the chain, but remember that it is the consequence that disturbs the supply chain performance and not the probability of an event.

2.3. Supply chain security

The aftermath to the terrorist attack at World Trade Centre and Pentagon September 11 2001 brought attention to the security in today's trade. The reasons are more than terrorist attacks. According to Closs and McGarrell (2004) three factors can be outlined. First, the globalization of the world trade which depends on and is generated by the free flow of people, goods and information. Second, the increasing demands from businesses for efficient supply chain operations. Third, the increasing threats 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 et al, 2004). The only problem with this definition is that it does not address the origin of the threat or risk occurs. 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 flipside of supply chain security is supply chain resilience, which is a supply chain's ability to withstand and recover from an incident (Closs et al, 2004). Supply chain risk should incorporate both the concept of security and resilience, where resilience also must handle a near miss incident, which could affect the performance of the supply chain from which it needs to recover.

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 anti-terrorism. Second, the focus is now to address 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 et al, 2004).

In the paper “Higher supply chain security with lower cost: Lessons from total quality management” by Lee and Whang (2003), they 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 in 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.

2.4. Security and risk management

Today risk is a factor in all business functions and processes (Cavinato 2004). This refers to 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 from both within the organisation and the environment. The search of minimizing the own business risk has always been a part of doing business. But minimizing the business risk often also leads to minimizing the profit from the business. Risk management contains different methods that strive to balance risk between profit and cost. This shall be compared with the use of security which in general terms means that an antagonistic threat needs to be minimized by using direct or indirect preventive methods.

Traditional risk management and security may appear to be congruent with each other. This comes from the fact that many security practitioners use traditional risk management methods. Traditional risk management methods are a good way to simplify and analyse complex problems like security issues. Further on, they are good methods for proper allocation of available limited resources to address unlimited risk sources to achieve a reduction of the total risk (Manunta, 1999). Most traditional risk management methods are based on statistics (achieved by various methods) and therefore traditional risk management methods 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 is the risk management approach for reducing disturbance. 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 or less non-linear. Therefore traditional risk management can not deal effectively with the dynamics of antagonism, which is the area for security. The causes for antagonism can be described as a spiral of inputs, processes and feedback, which explains the dynamics of antagonism. Such dynamics tends to make the analysis, assessment and decision very complex, and the world seems to be anything but deterministic (Manunta, 1999). Manunta here argues that security and traditional risk management are opposite to each other. This is a too limited view. Both approaches aim to reduce 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. The understanding of the antagonistic dynamics is vital for an analysis of where, when and how the protector shall be present to prevent adverse events from occurring. The security version of risk management needs to address the dynamics of antagonism by understanding the environment or the context of the threat. Therefore contextual risk management approaches are appropriate for dynamic risk sources, while statistical risk management approaches match static risk sources. Contextual risk management can be seen as intelligence, instead of equations, containing probability and effects, like in statistical risk management (Manunta, 1999).

This does not mean that traditional risk management can not be used in security work. It simply means that in security it is very important to first get a general 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, security is first of all interested in why and how an incident can occur. Both approaches aim to prevent and obstruct the incident itself and to limit the effects from it.

The difference between statistical risk management and contextual risk management can also be described by the lack of similarity, namely the nature of the threat from whom or what the protector shall protect the object. If the threat is antagonistic, then contextual risk management is the right way, while if the threat is predictable statistical risk management is the preferred method. Despite that, the two different concepts can be used together and to support each other. The difference between statistical risk management and contextual risk management can be illustrated with the differences in approaches and perspective. The statistical risk approach is based on statistical information and assumes some form of randomized predictability of incidents. The contextual risk management approach is based on contextual understanding and assumes some form of antagonistic threat and a nonlinear relationship between cause and effect. Contextual risk management is like statistical risk management aimed to reduce the total risk (cause and effect).

Everything that happens in a system that makes it vary from the ideal state is generating uncertainty throughout the system. In risk management terms this can be described as if the cause and the effect are known, then the proper countermeasure or the right plan of action can be used. If there is uncertainty within the system it will delay the starting point for the proper plan of action. Therefore uncertainty can be seen as a delay function 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 5.

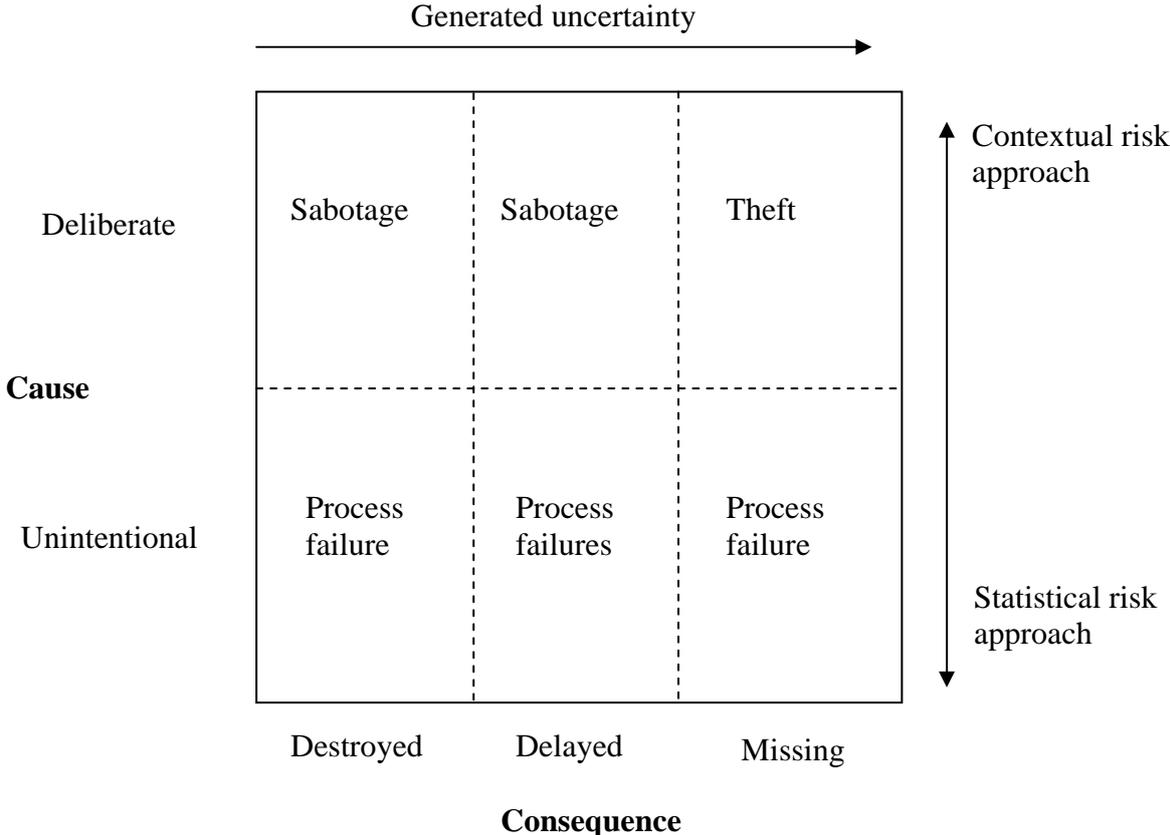


Figure 5: Cause/consequence matrix for cargo incidents

On the impact or consequence side of the risk there are basically three different outcomes, goods delayed, destroyed or missing, while on the cause side there still are deliberate and unintentional reasons behind the consequence. The most uncertainty-generating consequence

is ‘goods missing’. This is due to the fact that with the other two consequences it is clear what has happened and therefore the right action plan can be started. The missing goods can just due to a process failure or mistake be misplaced and will show up in another place than expected. The business impact will generally be higher if the goods are stolen or destroyed, than if they are just delayed (depending upon the length of the delay). But due to penalty fees between supplier and buyer the impact can be just as serious for a delay as for a theft. The real problem occurs when the own security or risk management capability is lower than the capability of the perpetrator. The difference between these two capabilities is the window of vulnerability (Almay, 2006). A proper risk management approach aims to reduce or hopefully shut that window.

Logistics literature agrees that uncertainty shall be reduced as far as possible (Nilsson 2006). The basis of this idea is that there exist equilibrium and stability in all logistics (Lambert 1998). In other words, everything can be controlled. But if the risk is caused by deliberate actions, then there is no stability. Nilsson (2004) states that with regard to uncertainty and complexity logistics researchers and practitioners need to “go with the flow” instead of trying to remove all uncertainty. In terms of supply chain risk management Nilsson implies that both a statistical (stable) and a contextual (complex) approach are needed in order to reduce the total risk. According to White (1995) risk analysis can be conducted in two ways, either holistically or reductively. The difference between these two ways is illustrated in table 7.

	Holistic approach	Reductive approach
Method	Systemic	Systemic
Issue tackled by	Investigating the problem’s environment	Reducing problem into smaller and smaller parts
Approach characterized by	An upward movement	A downward movement
Simplifies by	Taking multiple partial views	Breaking down problem into simplest parts

Table 7: Table of differences between holistic and reductionist approaches (White 1995)

The holistic approach is, like the contextual approach, useful when the risk arises from the environment and a greater understanding of the cause is needed to be able to reduce the total risk. Likewise the similarities between statistical and reductive approaches are useful, when the risk cause is repeatable and recurrently predictable. The antagonistic gateway is a risk that arises from both the interior and the environment of the transport network and is deliberately abused. Therefore the contextual or holistic approach is better to use than the statistical or reductive one. In this thesis this is achieved by focusing on both the potential perpetrator and the transport network and carrying out the analysis with theory from both criminology and logistics. This also means that this thesis does not attempt to break the problem down into its simplest parts, consequently it aims to perform and report a wide, multi-level analysis of the problem of antagonistic gateways in the transport network.

2.5. Logistics and transportation

Looking at transportation 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. Then 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 normally is to move material from one place to another. To be able to do this the material flow uses a flow of resources, meaning lorries, trains, airplanes and ships. These resources need infrastructure like roads, harbours, airports and terminals. This relation is explained in figure 6 (Wandel et al, 1995).

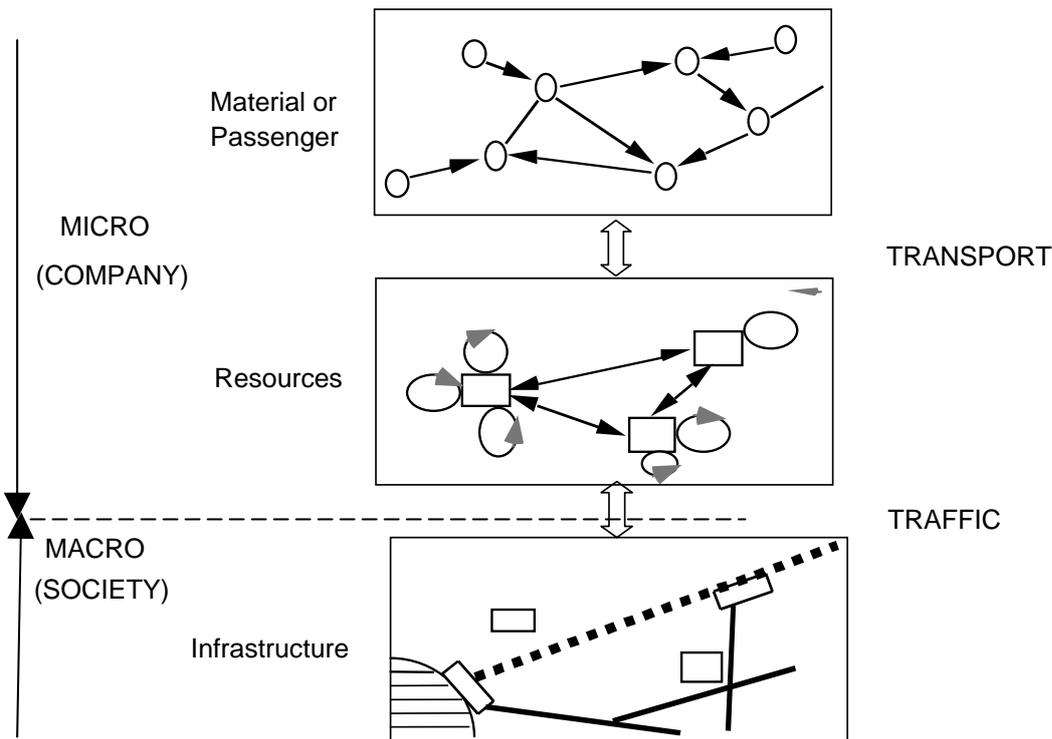


Figure 6: Levels of logistics (Wandel et al, 1995)

The complexity in logistics can be explained by displaying the four different flows that are always involved in logistics activities. The flows of material and resources are already mentioned. These two flows represent the “physical” part of logistics, but the other two flows are just as necessary to make the system work. First we have the monetary flow of capital that includes the payments in the system. When simplified, it can be said that the end user pays all. The last of these flows is the information transfer, which is vital to managing the system, because without information about the goods, destination, cost, means of transportation, route and delivery time the system will not work as expected (Lumsden, 2006). The four flows of logistics are illustrated in figure 7.

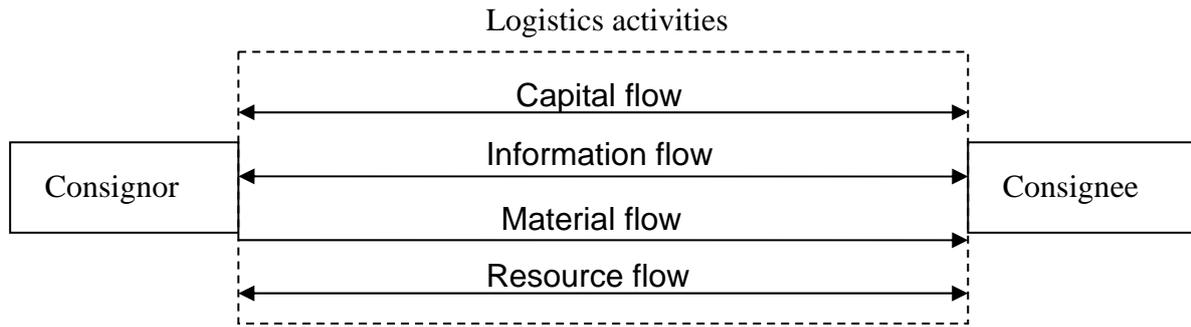


Figure 7: The four flows of logistics

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 means of connecting the nodes. Goods enter and exit the network through gateways, i.e. inbound and outbound gateways (Lumsden, 2006). Figure 8 shows a typical transport network with gateways.

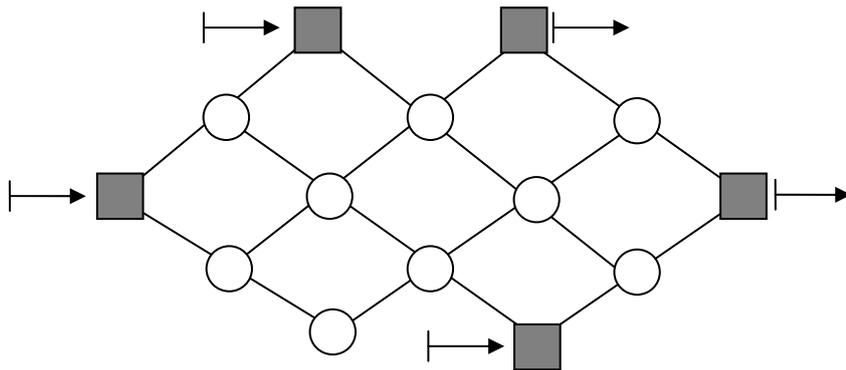


Figure 8: Transport network with gateways (Lumsden, 2006)

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 links in the network can be long or short. This means that from legal and practical reasons the network needs temporary stops in-between nodes. The legal reasons behind them are closely connected with society regulations on the cargo carrier itself. In road transport society regulates the allowed working time for the driver (a day, a week etc). The temporary stops close to a terminal or warehouse have an additional function as a waiting place for unloading scheduling according to the just-in-time principle. The scheduling of unloading in transport network terminals can depend on a shift in transporting modality (Kelleher et al, 2003). Therefore temporary storage is an important part of the transport network. The two different reasons behind temporary stops in the transport network are illustrated in figure 9.

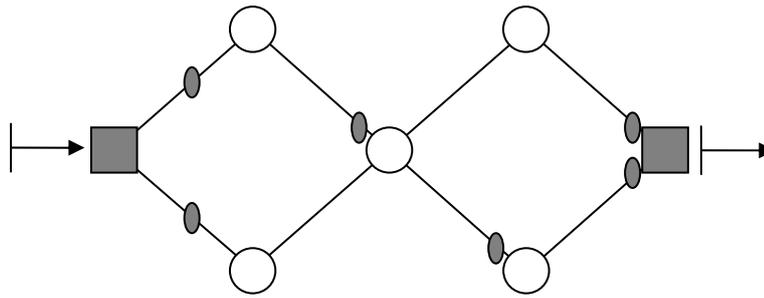


Figure 9: Transport network with temporary stops

The function of terminal-close temporary stops as time buffers in just-in-time distribution is closely related with the uncertainty of each transport. Normally there is a relationship between transport distance and the exact time of arrival. A longer distance (or longer freight 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 factory's internal activity or in other words, the demands from the receiver and not the forwarder or the consignor. Therefore the transport network needs temporary stops close to certain delivery nodes. This activity can be seen as an uncertainty reducing function in the supply chain. However, these temporary stops close to delivery points also bring another place for antagonistic threats to occur within the supply chain, and if an incident happens the uncertainty increases again.

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 basically 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 inbound logistics risk. The consignor outbound risk composites the uncertainty of the outbound gateway and the transport network process, as well as control and environmental risk sources. The uncertainty of the outbound logistics at the consignor must be reduced, in order to meet the need from the consignee inbound gateway, by scheduling in the transport network and the use of temporary stops close to the consignee. This is illustrated in figure 10 from a supply chain perspective.

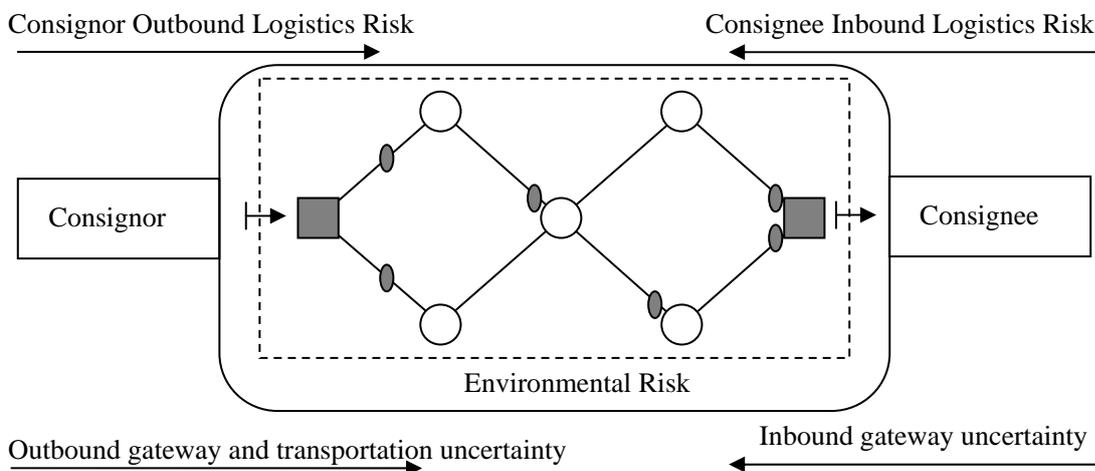


Figure 10: Risks and uncertainty in the transport network

The cause for why a transport does not deliver within the scheduled time-window can be either deliberate or unintentional. The important thing to remember with the use of time-windows is that they are there to smoothen the overall supply chain function and performance, by reducing the uncertainty between facilities within the chain. One of the causes for disturbance within the transport network, and thereby increased uncertainty, is antagonistic threats towards the freight itself.

2.5.1. Transportation and freight security

The security of freight transport was long under-developed, but when 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 (EU, 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 (EU, 2003). The technological development, as far as range and sophistication of anti-theft devices and after-theft systems go, is increasing rapidly. Especially attention is given to different tracking 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 different barriers in the business, is indicated by the following: Underestimated risks from the haulers' side; different standard in technologies; insurance companies do not always give premium reductions; technical standards do not yet exist (ECMT 2001 - b). These barriers and lack of cooperation can be patched up 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 on safe routes, parking areas with high security, precautions to take and appropriate equipment (ECMT 2001 - a).

The organisation TAPA aims through its two different certification programmes, Freight Security Standards (FSR) and Trucking Security Requirements (TSR), to improve transportation security. The FSR addresses mainly security issues on 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 acceptable security standards for assets travelling throughout the supply chain and the methods to be used in maintaining those standards (TAPA FSR). The TSR, on the other hand, address only security issues in road transport using lorries and are certified by self-assessment. The TSR specify 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 program to the FSR (TAPA). A transport network that is certified by TAPA can be illustrated like in figure 11. The square frames represent the general idea of FSR of 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.

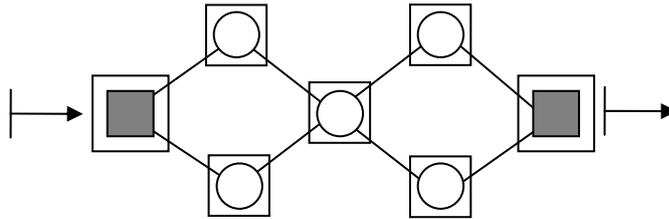


Figure 11: Security in the transport network

In transport security it is important to take an intermodal approach to avoid unwanted competition disadvantage between the various modes. This means also that the security methods need to be internationally accepted, at least 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 in-between other modes of transport are used. As a consequence of this, road transport needs a parking place near the intermodal terminal, if there is no waiting area inside the terminal borders.

2.6. Criminological theories used in this thesis

A definition of the scientific field of criminology is as Sutherland, Csessey & Luckenbill (1992) state.

“Criminology is 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 understood as the scientific study of crime, then it must always begin and end with a discussion of the term crime. This is achieved with the idea that there must exist a law to break if the action shall 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 all research in criminology (Sarnecki, 2003). This principle is decisive for this thesis.

2.6.1. 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 therefore is it valid to different extent for each and every person in each and every situation.

Modern criminology uses the rational choice theory as the basis of the research. This theory has its origin in the idea of the economical man, as comes from economic research. In short, the theory states that every presumed criminal shall be seen as a rational person, who makes decision about the potential crime from relationships between the benefits that the crime may bring and the troubles and risk it results in. By increasing the perceived trouble and/or the risks, is it possible with this perspective to reduce criminal activities (Sarnecki, 2003).

The opposite of rational choice is determinism. The idea here is that the course of events is completely depending on existing conditions. This approach refuses the idea of the own free will – everything is predetermined. In reality every individual is a mixture of influence ability and the lawful. Among social scientists today the idea of the 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, ethnical belonging or the society in which the individual lives, and how this affects his life with regard to the ethnical belonging, gender and social position (Sarnecki, 2003).

These two opposite perspectives to see the human being either as the master of his own life and decisions 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 it is also important with respect to the societal response to criminal behaviour (Sarnecki, 2003). It is commonly agreed that different types of crime demand different 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 (economical crime etc.), which are more rationally based. With this said, the big difference appears when discussing the possible punishment for a certain crime. If an individual is responsible for his own actions (rational choice), then the possible punishment, will have a deterrent influence. But if the individual is a victim of circumstance (determinism), then it is useless to punish the individual. Therefore

all crime prevention methods assume that each 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 estimate the risk in a rational way. An individual, who previously has received a formal or believed punishment for an action, should be less likely to commit that action again. The outcome from a formal punishment on perception of risk is mixed (Horney. et al., 1992), therefore each individual should be considered not rational, but to act rationally on the margin.

2.6.2. The 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). The elements are:

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

It is clear that the first element is the actual offender, while the other two elements describe the object or target and also the protection of it. It is important to remember that a crime occurs when all three elements are fulfilled and that it is the perpetrator who decides if the object is suitable, and also whether the capacity of the guardian has a deterrent influence. With other words, the perpetrator evaluates the situation or system by using external and internal variables and then decides how he will act.

2.6.3. Opportunity to crime

Crime opportunity is a cornerstone in all 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 ten crime opportunity principles are self-explanatory and easy to understand. All these principles are valid for every type of crime and therefore are them also valid for crimes committed to the transport network. The more interesting principles of those opportunities will be explained and described later in this thesis. The most important to remember with crime opportunities is that an opportunity alone does not explain why a crime occurs. A crime will need both 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 needed opportunity or incentive depends on each individual person.

2.6.4. Routine activity perspective

The fourth of the ten crime opportunity principles states that “Crime opportunities depend on everyday movements”. This can be reformulated as crime opportunities depend on routines or predictability within certain boundaries. This rephrasing also includes more principles than the stated one, implying that system predictability or routine provides crime opportunities. This is called the routine activity perspective in criminology (Cohen et al, 1979). The theory is a strong theoretical foundation to understand crime and opportunities for crime. The routine activities perspective argues that normal movement and other routine activities play a significant role in potential crime.

The transport network is made up of basically three levels (see chapter 2.5), infrastructure and the flow or movement of both 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 is also to a large extent predictable. The routine activity perspective states that the predictability in infrastructure and resource movement will significantly contribute to 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 therefore provides a theoretical foundation regarding antagonistic activities against the transport network. Thus, when the transport network changes, so does the theft opportunity.

2.6.5. 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. Situation 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, the potential payoff, and the 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. 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 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 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). 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):

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

Increase perceived risks (Clarke, 1992) – If perpetrators think that they will get away with a theft, it is more likely that they will commit it. By increasing the risk for perpetrators they are less likely to commit a theft. This can be accomplished by using 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 the potential perpetrators. This can be accomplished by either 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, as follows (Clarke et al, 1997):

Inducing guilt or shame – A theft is more likely to occur if it can be excused by appeal to reasons like “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 ethnical relativity. Companies and organizations can affect this ethnical relativity by using company rules, signs and regulations that demonstrate the right moral values. When theft is seen as an additional wage benefit for the employees, this preventive action has failed (Muir, 1996). By appealing to people's moral and making it easy for them to do the right thing, then excuses will be more difficult to use (Clarke et al, 1997).

2.6.6. Crime displacement

The theory of crime displacement predicates 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).

Crime displacement assumes that crime is inelastic (Repetto, 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 (Repetto, 1976).

The perpetrator has mobility (Repetto, 1976) –The perpetrator has flexibility relative to time, place, method and type of crime to commit. In reality, perpetrators are normally limited in their mobility, adaptability and flexibility relatively 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 criminal 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 perpetrators 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 can not be eliminated but rather they can be reduced by implying substantive preventive countermeasures. The object is to reduce crime opportunities which will lead to a change in all potential theft situations and therefore crime displacement is a valid theory (Repetto, 1976).

Crime displacement can occur in several ways. Repetto (1976) uses five types of displacement – crime, target, method, place and time. Barr and Pease (1990) add another type of displacement, namely the perpetrator. Thus, 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 to them than others. Furthermore, it does not explain what are 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 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 perpetrators ability to organize a successful crime and their relationship relative to the actors within the transport network that are the fundamental variables to categorize perpetrators.

2.6.7. The professional vs. the opportunistic perpetrators

Based on this fundamental categorization, there are basically two types of perpetrators; the *professional* and the *opportunist* perpetrator (Klemke 1992 - A). The professional perpetrator is an offender, who 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 about the unpredictable elements in the security system, for example another human, than the technology. This all depends on the perpetrator's knowledge about the security system's strengths and weaknesses. A professional perpetrator can also acquire the required technical expertise to overcome any predictable countermeasure (Kallis et al., 1985).

The opportunistic perpetrator steals an item because that item 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 any security system at any specific location. The presence of visible security measures instills a feel of fear in the potential opportunistic perpetrator (Beck. 2002).

2.6.8. Internal or external perpetrator

The position of the perpetrator relative to the company or organisation, in which a perpetrator commits a crime, is of great importance both 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, thereby increasing the possibility of a successful crime. The transport information can be given to an external perpetrator by an employee. The external perpetrator can also retrieve the required information, either by hacking into the transportation computer network or by employing non-criminal tactics like 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% 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 perpetrator acts not random or unstructured but more a response to social and environmental factors that are present in the work environment (Tryon et al., 1997). According to Speed, it is useful to divide employees into four different categorizes, depending on duration of employment and age (Speed 2003). This categorization can be used to assist in segregating potential dishonest employees and thereby 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 12.

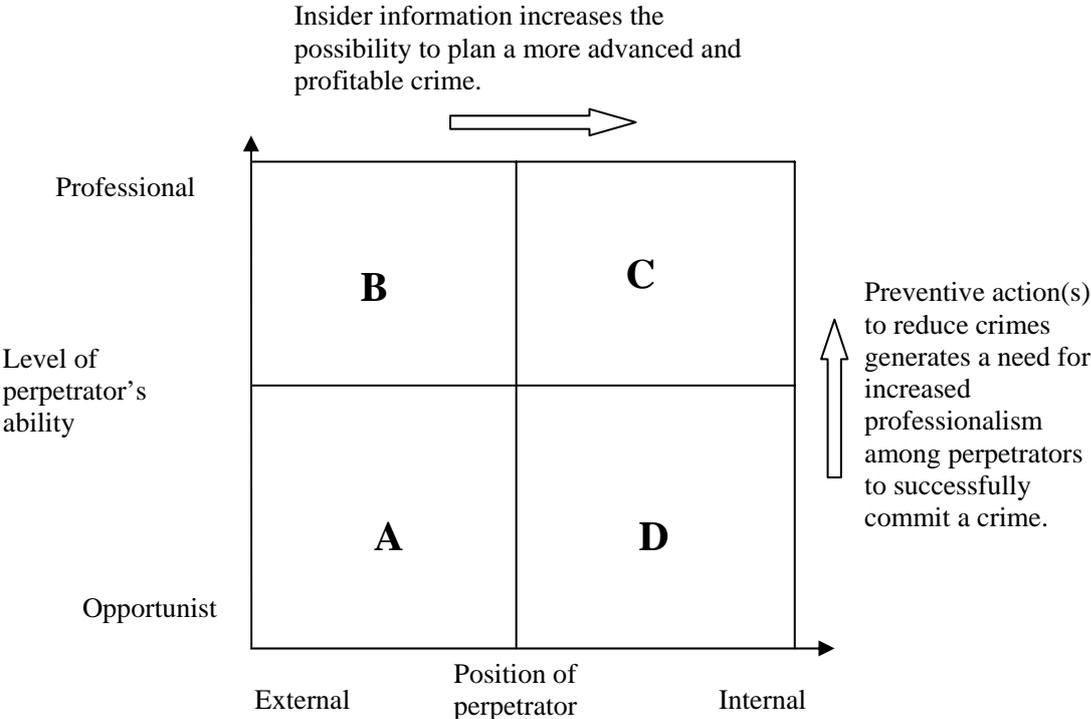


Figure 12: Perpetrator's characteristics matrix

The following are relative crime examples in figure 12:

A: Shoplifter; walking past a parked, open and unattended a 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 choices of if, where, when and how to commit the cargo theft. This means that if a single part of the network implements some countermeasures in an attempt to prevent crimes, then the crime displacement theory predicts that criminal activities will change to another part of the network.

2.6.9. Security, risk management and crime prevention

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 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.

Security for an individual or a group of individuals can, if it is unrestricted, even jeopardise the security for others by threatening them or transfer threats onto them. This type of discussion can be found at philosophers like Hobbes and Mills. An unbounded or unrestricted individual security could threaten the authority of a state. This problem can be illustrated with the current debate about individual and private secure communication encryption, which some states want to make illegal, unless they can break them. All this comes down to that a security problem may or may not be a legal problem. Security, as an idea, can be explained with a protector or guardian and what threat it tries to protect the asset or object from. This threat can be from both sides 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 (see chapter 2.4).

Contextual and statistical risk management approaches as crime preventing methods work in different way and address different types of potential perpetrators. This difference refers back to the difference in the philosophical view between contextual and statistical risk management. Statistical risk management needs a fairly predictable world or at least a larger amount of trustworthy statistics. Because previous events or incidents are the basis of statistical risk management, it can not 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 use unsophisticated and indifferent methods that are based on opportunistic behaviour (Manunta, 2002). But, as potential perpetrators become

more and more sophisticated and with larger capability, the predictability in terms of statistical prediction will reduce dramatically. The antagonistically acting 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).

2.7. The deductive framework for this thesis

This framework is deductive and aims to combine the two scientific fields of logistics and criminology from a logistics perspective. Therefore, theories from criminology are used to support, amend and explain theories from logistics.

2.7.1. The supply chain perspective

The supply chain is a network of autonomous or semiautonomous business processes that produce physical goods or services for customers. Not all products or services are legal though. The end-user, for whom the entire supply chain exists, normally wants some kind of discount, if the end user knows that the product is illegal. This situation then leads to that the illegal actors try to appear legal. Depending on the production/acquisition question based on the illegal side of business, supply of illegal products is basically achieved by either theft or illegal production. The distribution of these products is achieved through logistics. This thesis addresses the problem with illegal products entering and legal ones exiting the legal transport 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. 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. This is illustrated from a supply chain perspective in figure 13.

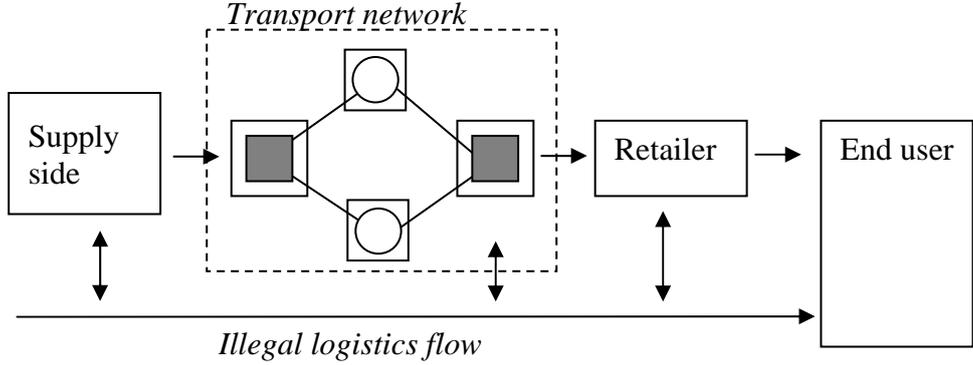


Figure 13: The supply chain perspective with gateways between logistics flows

The supply side box in figure 13 includes activities like manufacturing, assembling, raw material production and so forth. From a supply chain perspective, these gateways can appear in each one of the complete processes. The probability for and economical impact from the usage of these gateways can be seen as parts of supply chain risks but with completely different effects on supply chain performance. The smugglers do not want to draw extra attention to their business, therefore they do not primarily decrease the supply chain performance, however, several countermeasures do that. The cargo thieves, on the other hand, decrease performance and contribute to disturbance in the chain. Depending on this difference and that both types of perpetrators act from a rational choice perspective, they will try to maximize their business objectives. This may lead to that they move the gateways to another part of the supply chain. This thesis addresses only the gateways that act and appear in the transport network.

2.7.2. The transport network perspective

The physical flow of products through the supply chain is conducted by a transport network. The risks and uncertainties that exist within the supply chain also affect the transport network. A disruption in either inbound or outbound logistics can affect the overall performance of the supply chain. All freights within a transport network are to some extent scheduled according to various reasons; one of the most common is the need from the consignee terminal for delivery within a certain time-window. 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 need from the supply chain for a scheduling of all transport activities also provides crime opportunities, according to Cohen and Felson’s (1979) theory of routine activities perspective. The rigid scheduling in the transport network provides an excellent breeding ground for recurring crime opportunities. Crime opportunities in the transport network can also be seen as antagonistic or informal inbound and outbound gateways, where an antagonistic inbound gateway is smuggling and the antagonistic outbound gateway is theft. Sabotage is an antagonistic outbound gateway without removal of the goods.

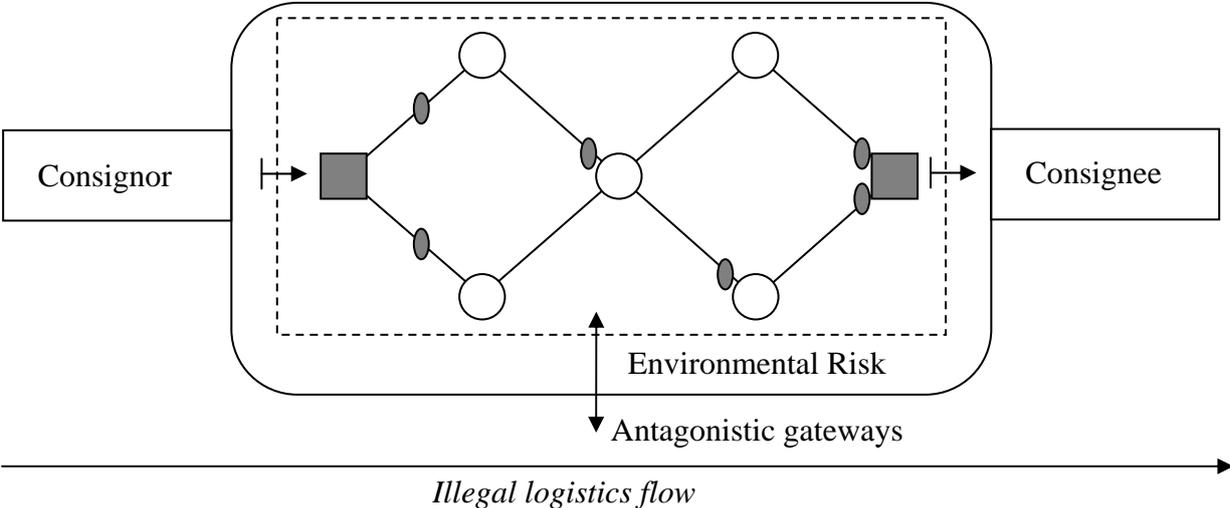


Figure 14: The transport network perspective with antagonistic gateways between systems

The opportunity for a crime is together with a motivated perpetrator, needed for a crime to occur. The transport network can seldom adjust the object’s suitability itself (while the supply chain can), but it can adjust the presence of guardians. 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.

The potential perpetrator, who acts from a rational choice perspective, will use a personalized decision process about the potential crime from relationships between the benefits that the crime brings and the troubles and risks it results in. The creation and usage of antagonistic gateways is therefore also a subject for a benefit/trouble-risk decision process from the potential perpetrator’s side. Transportation security therefore aims to alter the outcome from the potential perpetrator’s decision process regarding the usage of an antagonistic gateway.

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). This means that within the potential perpetrator’s capability, he will try to find a

different antagonistic gateway to exploit. The mission to make the entire transport network securer can be described as an increasing security level or a harder/riskier shell surrounding the network. This can be called transport pipeline security which enhances both terminal and freight security. In figure 15 the current general view of the transport pipeline security within the transport network is illustrated.

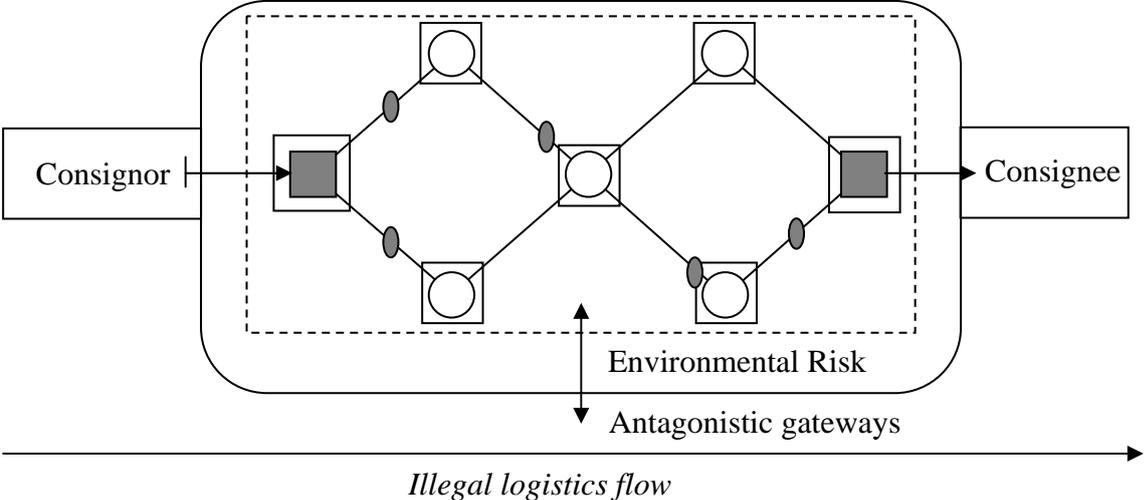


Figure 15: Transportation security in relationship to antagonistic gateways

The perpetrator’s decision process is the key issue to understanding usage of antagonistic gateways in the transport network. The transport pipeline security methods need to be based on an understanding of this decision process, the antagonistic dynamics of potential perpetrators. This understanding is to a large part also an understanding of the context in which the perpetrator acts. The difference in perpetrator context is easily described with the difference between regular cargo thieves and ideology-driven perpetrators, such as terrorists. The thieves are after the money that the cargo will give them, therefore they want to steal high-value, untraceable and highly demanded products. The ideology-driven perpetrator wants to make a statement with the attack, therefore he wants to sabotage products which will give the statement attention and also (if possible) understanding for it. If a potential terrorist wants to finance an upcoming terrorist attack by a cargo theft, the perpetrator will act as a regular cargo thief. This difference in perpetrator context is vital for applying the right type of countermeasures in the transport network. Transport pipeline security against these types of antagonistic threats in the transport network aims to alter the contextual perception of the network and thereby reduce the problem with antagonistic gateways.

3. Methodological framework

This chapter introduces the scientific approach and its application in the research.

3.1. Research procedure

The research carried out in this thesis can be described as a step-by-step process. The framework of this thesis has therefore been developed as a result of empirical findings and theoretical insights. The research is characteristic by a continual development and validation of the framework for this thesis. Validation has been accomplished by presentations for and feedback from several different experts in the field. This process has been conducted several times. Therefore it is difficult to state if the theory or the empirical data came first. In terms of theory of sciences, this research procedure is neither deductive nor inductive. The research procedure has been governed by the need for a deeper and clearer understanding of both the general problem with criminal behaviour in the transport network but also with a research question centred view on what was important during the research process. The research procedure for this thesis can therefore be categorized as abductive (Dubois et al, 2002). This thesis is written according to the idea of first developing a general theory based on other theories and observation, using a deductive approach. The papers in this thesis shall be seen as an inductive method, in order to prove the deductively developed theory (Kekäle, 2001). The deductive approach helps to substantiate the objectivity of this 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 like economics, philosophy and organization theory. The interdisciplinary exchange of views, ideas and theories is needed in order 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 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 standpoint by illuminating several areas of interdisciplinary research in logistics during the past. One exchange area that he does not address explicitly is the one used in this thesis, namely the logistics and criminology interaction. Stock also draws the conclusion that logistics will continue to borrow theories and ideas from other disciplines, as it is developing as an own scientific field. This thesis can be seen as a confirmation of Stock’s conclusion.

3.2. System approach

The research in this thesis follows the tradition in logistics to use a system approach to answer the research questions. The system approach also implies a top-down perspective on the system. The system approach in this thesis uses two separate systems that interact with each other. Those two systems are the legal (white) and the illegal (black) transport network, which both are parts of legal and illegal supply chains. Transported products must be a part of either the legal or the illegal system. This is a simplification done with the purpose to illuminate the

illegal exchange of products between the two systems. In reality the exact system affiliation can be hard to establish, then the term “grey market” is often used. In this thesis grey logistics is inbred as a part of the black system.

The system approach allows logistics to be seen as more than the sum of all activities. Logistics is seen as a whole system with functions or parts that interact with each other in ways that make them more than just the sum of them all. There are two attributes that distinguish a system; its boundaries and the context in which is presented (Wilson, 1990). The different models and theories from supply chain management and logistics that are used in this thesis do not have a legal aspect to them, but as they are presented by their authors, it is implied that they are developed from and for the legal logistics system. The reason does not make them invalid for illegal logistics system. The explanation is found in the context to the two systems. Both black and white supply chains aim to fulfil end users needs, with regard to product, price and place. The promotion aspect is mainly used by the legal system but the black systems can abuse market activities by supplying branded products that get their branded status from legal branding activities.

The majority of all complex systems indicate a large amount of redundancy and by using this redundancy is it possible to simplify the system and thereby both gain understanding and the ability to control it (Waidringer, 2001). In this thesis this simplification is achieved by using the same theories from logistics to describe both systems. The difference between them is instead found in their respective context of legality. This context difference affects the configuration of the two systems, in a way that the same variable will receive different importance. The main idea behind a system approach is to understand not only the different components or parts of the system but to understand their interaction with each other 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 with more than one real case. System analysis and construction are a part of the developing process for system theory.

The system theory used in this thesis follows Arbnor and Bjerke’s approach. First two different and imagined systems were created and described in a model. The purpose of this model was to illuminate similarities and differences, for both internal and external factors. The complexity of these two systems was then reduced by the removal of redundancy in each model. The last step was to describe the interaction between them, make the legal logistics system the main system and appoint the illegal logistics system as the parasite that abuses that host system.

3.3. Research process

The research process began with a literature review, of both previous research in the field and research in related scientific fields, to get a deeper understanding for the subject and to generate ideas for the research presented in this thesis. Based on the literature study, a methodological strategy was formed. This strategy can be described as an abductive approach with a main focus on understanding both the business itself, the problem with criminal

activities against the business and the interaction between the logistics business and the criminal activities.

The research presented in this thesis is based on five different studies that were conducted during a four-year period. They can be categorized according to the general purpose of the single research. These categorizes are exploratory, descriptive and explanatory. According to Yin (1994) it is generally believed that each research category has different methods, i.e. where an exploratory study uses cases studies, a descriptive study uses the survey approach and finally the explanatory study uses an experimental approach. Yin argues that these types of methods are not locked for use in one particular category of research. They can all be used to strengthen each other and in different combinations.

The research process started with an exploratory study. The meaning was to from the outcome of that study form a more precise problem definition (Hellevik 1984). This study formed new and more precise research question that gave directions for three more exploratory and also descriptive studies. In direct relation with writing this thesis a fifth study was conducted as a descriptive survey. Table 8 illustrates the different research strategies used in studies related to this thesis.

	Exploratory	Descriptive	Explanatory	Normative
Study 1 (Paper A)	X	X	X	
Study 2 (Paper B)	X	X		
Study 3	X	X		
Study 4 (Paper C)		X	X	
Study 5		X	X	

Table 8: Classification of the five studies

The first three studies were mainly conducted in order to understand the problem and cargo crimes in logistics business but also to describe how the interaction between the business and the problem evolved. Studies 2, 3 and 4 were all based on outcomes from study 1. The fourth study was closely linked to study 3. The fourth and fifth study were, different from the other three, more systematic. They were not conducted to explore the problem area but to describe it instead. The relationship between the five different studies and how they affected each other is shown in figure 16.

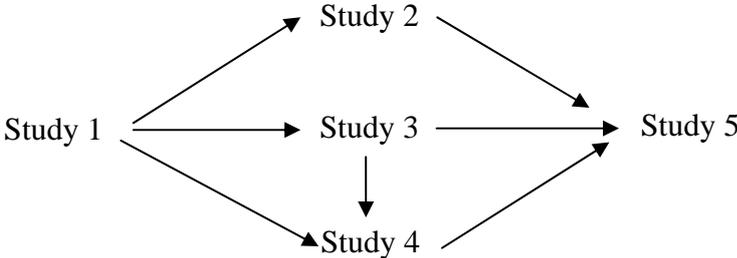


Figure 16: The relationship between the five studies conducted in this thesis

During this process the three papers in this thesis were written. Paper A (study 1) addresses the problem with cargo theft, an outbound antagonistic gateway in the transport network. Paper B (study 2) takes a closer look at the inbound antagonistic gateway and the relationship to the legal transport network. Together paper A and B cover the problem with interaction or exchange of goods between the legal and the illegal transport network. Paper C (study 4)

addresses the need from the transport network to retain and use the so-called weak spots found in paper A. Study 3 and 5 are not presented as papers in this thesis, but referred as follows: Study 3 is a written report in Swedish and study 5 is presented partly in the result chapter.

During the research process study 1 or paper A has received the most interest, due to the fact that as presented in figure 16 the outcome of that paper is essential for the whole thesis. The research process for paper A was the longest one. The study started with six interviews with persons experienced in the area of theft prevention within logistics. Based on these six interviews a deductive hypothesis testing process began to find the right mix of theories that match the outcome of the interviews. During the research process different hypotheses were presented and discussed with several representative persons within the research area. Their comments, ideas and suggestions were all taken under considerations and used in the next step in the deductive hypothesis test process. The same process type has been used in the other four studies. The main reason for the use of this type of process was the lack of reliable information, both primary and secondary, that otherwise would have been a bigger problem than it now was.

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

- Companies are reluctant to state in official information channels that they have problems with criminality. This is for business reasons like imagined “bad will” from potential customers.
- The growing use of company boundaries and insurance companies to limit the economical consequence of an incident has reduced the companies’ willingness to address the actual problem instead of the economical effect from it.
- The lack or imagined lack of interest in this problem from the legal system has contributed to reduce the 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 about the criminal activities indicate that a qualitative approach will be needed to get a better understanding for the problem with criminality against cargo flows.

All business involvement in this thesis has been affected, to different degrees, by the five above-stated reasons for reliability of the information about criminal activities. Therefore all companies and organisations have been granted anonymity in their contribution to both the research and the results in this thesis. All companies and organisations, which have been involved more than once or in any of the five studies presented in this thesis, are mentioned in appendix 1.

3.4. Data sources and their reliability

The validity and credibility of the research depends on the use of data and the sources for this data. The data sources are normally divided into primary and secondary sources. The primary sources are interviews and the secondary ones are literature, databases and the internet. Interviews can be executed in several different ways. In which way the researcher chooses to conduct the measurement and data collection, depends on the aim and purpose of the research.

In this thesis the scope has been to understand and to enlighten the antagonistic gateways between the legal and the illegal logistics systems from a supply chain perspective.

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

Regarding secondary data, it is always important to ask one-self where the data comes from and how it is collected and analyzed. The main problem with secondary data is simply explained with the question 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 complete research. The secondary data and information in this thesis are used only as a trend indicator and not as a standalone answer to any research questions.

The information about the black logistics is all from official reports and interviews with security personnel or personnel with similar assignments. This means that the black logistics description is based on secondary data instead of the preferred primary data. This is due to that primary data is very hard to get. 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). The secondary data from reports that is used is collected by trustworthy institutes like FBI, DEA, Europol and the European Commission. In some cases the report is from a trade association, but this occurs only for counterfeited products.

The interviews are made with the purpose of getting examples of black logistics that uses the white logistics flow. The problem here is that the only examples that are mentioned are those which been discovered and not those which escaped. This implies that in real life undetected black logistics remains better than described in this thesis, because the description mainly uses examples that are failures, in one way or another.

3.5. Interviews

All interviews conducted in relationship with this thesis are made in the same way. The interviewees all had long recorded experience of both the logistics business and of theft prevention. They represent different aspects of stakeholders in logistics, both today in their present positions and also with their experience from previous employments. 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 all interviewees were guaranteed anonymity, so that they would not fear reprimands from their employers. The interviews were all ended with a mutual survey of the notes taken during the interview to ensure that they were representative for the interview (Mishler, 1986).

3.6. Verification and validation of results

Validity and reliability of the research are two different factors that intend to verify the results from the research process and assure the credibility of the research. Validity means that the chosen methods really measure what is intended. The problem to achieve valid information or data is less in qualitative methods or analysis than in quantitative methods. The reason for this is that qualitative methods give a certain nearness between the researcher and the subject. This nearness is not free from problems, because it means that the researcher and the subject influence each other. To avoid the interaction between researcher and subject the researcher needs to be aware of how he affects the subject and then take that into consideration during the research process (Holme et al, 1997). Validity can be further separated into internal and external validity (Yin, 1989). The internal validity aims to establish a causal relationship, to show that conditions lead to other conditions by pointing out the distinguished relationship between the conditions. The external validity aims to establish a domain where the result of the research can be generalized. The internal validity is achieved with the theoretical framework and the external validity is accomplished by the three papers that are a 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. The reason for this is that qualitative methods are used to understand certain factors and courses of events. But quantitative methods emanate from statistics and are therefore more sensitive for random factors (Holme et al, 1997). A good way to achieve high reliability is to use obvious and clear questions. During an interview is it important to give the interviewee all the time he/she needs and that the interview is conducted in an environment where the interviewee feels safe. The reliability of this research is achieved by all interviews being based on simple questions and conducted in a descriptive way. All interviews have been executed by the author.

4. Results

The theories presented in the framework in this thesis are in some ways used in one or more of the three papers. The results from all five studies conducted in relationship with this thesis are related to the three research question as follows:

	RQ1	RQ2	RQ3
Study 1 (Paper A)	X	X	X
Study 2 (Paper B)	X	X	X
Study 3	X	X	
Study 4 (Paper C)	X	X	X
Study 5	X		X

Table 9: Relationship between the three papers, the two other studies and the research questions in this thesis

4.1. Link between appended papers and the two studies

This thesis addresses the in- and outbound antagonistic gateways to the transport network. All five studies address at least two of the three research questions in this thesis. Paper A and C are also related to the third research question as well. Together they contribute to the credibility in the research and also provide an image of the complexity within this research area.

Paper A has double 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 a first explorative view about 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 in Paper B: The purpose of paper B is to analyse the similarities and differences in the design of logistics systems with respect of the legality of the transported goods. This means that the legality of the goods is a vital factor when it comes to taking the goods from their point-of-origin to the customer. By means of a systems analysis approach, based on cases and supply chain theory, this paper discusses the elements that constitute the respective logistics systems design due to legality. The work with paper A and B has been conducted more or less simultaneously and therefore they look at the problem of antagonistic gateways in the transport network in different perspectives. Paper A looks at the outbound antagonistic gateways while paper B addresses the problem of inbound antagonistic gateways.

The research conducted in study 3 was related to the need and design of a secure parking space for road transport. This is linked back to paper A by the fact that more than one of the interviewees pointed out parked lorries as a easy target for the potential perpetrator to steal from. The outcome from study 3 was published in a report (Dillén et al, 2006). The result in that report formed together with the explorative view of the problem with antagonistic gateways, the interesting question, why do we need these parked lorries? This becomes the research question in Paper C.

The main result from study 3 is that the extended usage of parking spaces for lorries during road transport has become a big problem with crime as theft of cargo and/or lorry. The development of the problem differs in different parts of Europe. The study was limited to Sweden with a European outlook. The general trend in Sweden for crime against the transportation business is that it has decreased but the place has changed from the terminal to the links in-between them instead. The same conclusion was drawn in paper A. These two studies (1 and 3) used different sources of data, both in form of interviewees and statistical information. Therefore, based on information retrieved during study 1 and 3, is it likely that the trend regarding the usage of antagonistic gateways against road transports is shifting from a terminal problem towards a freight problem. These trends were in study 3 the main issues and led to the discovery of other trends. The general conclusion from paper A was that the theory of crime displacement is valid for cargo theft and smuggling. This conclusion, together with the trend revealed in study 3, pointed out the parking spaces as the new weak link in the transport chain. This combined conclusion formed the research question in paper C.

Paper C addresses the problem of antagonistic gateways in the transport network's perspective and explains why certain network characteristics can not be changed without changes in the supply chain characteristics. It focuses on the need from the supply chain for the temporary storage to function as a disturbance neutralizer and thereby reduce risks and uncertainty from within the supply chain. But the temporary storage areas close to receiving terminals provided the potential perpetrator with a recurring crime opportunity which also becomes the weakest link, in relative terms. Therefore, in order to reduce the total risk for the supply chain, it is needed to reduce crime opportunity in the temporary storage area.

The conclusion in paper C shall be compared with the findings in paper B. Where paper C states that the predictability of the transport network is vital for the legal supply chain, paper B states that the predictability of the transport network can be abused for smuggling purpose. Paper B shows that the decisive difference between black and white logistics is found in information about the products, transportation routes, ownership and different domestic laws. In terms of discovering illegal goods in legal logistics flows the need for correct information can not be overestimated. The pure nature of the illegal goods governs the choice of logistics setup, concealed shipment or own system. The more difficult it is to establish if the product is illegal or not the more likely is it 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.

The fifth study is designed to be descriptive and explanatory for the conclusion drawn in chapter 2, but also as an indicator for future research in relation to this topic. The fifth study was conducted as a survey study using 20 statements to describe the usage of antagonistic gateways. The 20 statements had closed-end answer options for the 30 organisation that were involved in the survey. The involved personnel had job descriptions as security officers, claims adjuster and criminal experts. This study also contains interesting combinations of questions, which together clearly illustrates the complexity of this topic.

The outcome from the fifth study clearly indicates that the different theories from criminology used in this thesis are valid and contributes to the result. The study also provides valid arguments for that the interaction between theories from logistics, risk management and criminology are decisive for the credibility of this thesis.

4.2. Paper A: Cargo theft from supply chains: Crime displacement in logistics

Where there is a logistics flow there is always a risk for having the goods stolen. If this risk source for disturbance in the supply chain is not taken seriously, it will increase, in the long term, the cost for the supply chain. This disturbance can have two different effects on the flow, namely stoppage or drainage. It is the stolen volume in relation to the total volume that determines which one of the two effects a cargo theft will bring to the chain. 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, he will do so within their own mobility and ability. This is crime displacement in the transport network.

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 decline in the number of thefts would be 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 has also increased. This trend demonstrates that the perpetrators steal the goods in order to convert it to money. That perpetrators are becoming more professional is a general statement about cargo thieves. Correct countermeasures alter the potential perpetrators' decision process in a way that simply can be described as that the perpetrator will seek the weakest point within their mobility and ability to continue with thefts.

The theory of crime displacement in the transport network states that within the potential perpetrators' mobility, they will change their criminal pattern in response to countermeasures implemented by the business. The six displacements are the result of a change in the total theft situation, especially after a change for the purpose of preventing crime, which generally is implemented to reduce theft in a special part of the transport network. The preventive action also forces the perpetrators to become more professional in their criminal activity, so that they still may be able to commit successful cargo thefts. The result is a direct correlation between preventive countermeasures, the potential perpetrator's reactions and the need for an integrated system approach in order to obtain an absolute reduction of cargo theft incidents. The theory of crime displacement in the transport network explains why the absolute reduction is hard to achieve if an integrated systems approach is not used to secure the effectiveness of countermeasures for the whole supply chain.

4.3. Paper B: Differences in Black and White Logistics Systems Design

All transport or logistics activities can be divided into legal and illegal ones. The different activities together form systems of black (illegal) and white (legal) logistics. One big problem is the grey area between black and white logistics that is made up of different regulations in different countries and limitations in volume depending of the ownership of the goods. This problem is best illustrated with drugs and medication like growth hormone, which is illegal for almost everybody to own and possess, but for medical purposes it is legal both to own and to use. So depending on who is the owner and forwarder, growth hormone can be in either black or white logistics.

This paper shows that the decisive difference between black and white logistics is found in information about the products, transportation routes, ownership and different domestic laws. In terms of discovering illegal goods in legal logistics flows the need for correct information can not be overestimated. The pure nature of the illegal goods governs the choice of logistics setup, concealed shipment or own system. The more difficult it is to establish if the product is illegal or not, the more likely is it to be transported in the white logistics system. By using or stating reliable false information to the white logistics company, it is possible to raise the likelihood for the illegal shipment to reach its consignee. Whenever an illegal product is entering the white logistics system, there is a cross-over point between the two systems. To prevent this from happening many different methods are required, but common for all methods is the effective use of information. If not prevented, the black logistics will continue to parasite on its reluctant host. The general reaction of white business to reduce black logistics activities corresponds well to the four flows of logistics. The use of RFID and other types of unique identification on every single product increases the possibility to track stolen goods and makes it more difficult to produce counterfeit products. This strategy could open for the possibility that customs, police and other authorities easier can find counterfeited products. This requires extended co-operation between different stakeholders. The last type of reaction is the CSI which makes both the resources and the infrastructure more secure, simply by making it riskier to transport stolen or counterfeit goods using containers. The biggest contribution that CSI brings to security is its focus on the flow of information and that the information about the shipment is correct. This problem was illuminated in all five cases, which shows how important it is to have the correct information about a shipment. In other words, information is the key to unlock the cross-over activities between the black and the white logistics systems, but if the information is used in a wrong way or insufficiently the black logistics only adjusts and continues the illegal business as before.

4.4. Study 3: Crimes against commercial traffic (Dillén et al, 2006)

The parking areas along the European road network are insecure to use. Crimes against drivers, lorries and cargo constitute a growing problem. Lorries that are standing still fully loaded are interesting robbery objects. The Swedish National Road Administration has felt a growing concern about the extent of this problem and its development in Swedish parking spaces. The purpose of this study was to analyze the need and demand for secure parking. The main focus was to map the extent of the problem of cargo-related crime on parked vehicles in Sweden. According to the organisation Eurowatch the losses due to theft of goods during transportation were €225 millions in 2004. Furthermore they add that the police consider the actual losses three times as high. At a European level there is no coordination and there exist

no cumulative figures about the true extent of the problem. The desired goods are above all electronics, clothes and shoes, but also food, alcohol and tobacco products. During recent years the number of burglaries in lorries have increased constantly. The break-in occurs mainly during night time when the lorries are parked. At several occasions the driver has been asleep in the cabin. The goods themselves are not the only target, in some countries in Europe one percent of the cargo-carrying lorries become stolen each year. Trend analysis indicates that the problem increases.

The general trend in Sweden for crime against the transportation business is that it has decreased, but the place has changed from the terminal to the links between them. This development may be explained by that the physical security at terminals has improved. This is achieved with the implementation background checks on prospective employees, training, security policies and of course different technological solutions like CCTV, access control systems etc. The problem with lorries and cargo theft is without any doubt severe for goods owners, forwarders, haulers and the police. Nevertheless the police do not necessarily prioritize these types of crimes. This is especially true when it comes to gathering and analysing information about the problem. The insurance business needs to take its responsibility and demand better security. The excess and the premium for insurance are today too low to force the business to enhance its security. The buyers of the transportation need to become more explicit in their demands on security during transportation.

The report is based on information on a small part (mostly information from Sweden regarding the Swedish situation) of the problem with cargo theft. The trend found presented in this report indicates a clear increase in both value and actual incidents with cargo theft during road transport. The use of violence from the perpetrators is not as common in Sweden as in some other parts of Europe. To continue the work the different actors and stakeholder must rally around a mutual strategy to prevent cargo theft. The pure extent of the problem clearly shows that international cooperation and solutions are exceedingly important.

This report was also presented at the Transport Research Arena conference in Gothenburg in June 2006 by the author of this thesis (TRA 2006).

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

The demand on high supply chain performance today, together with higher awareness about supply chain risks and uncertainty, has increased largely in recent years. The purpose of this paper is to analyze the role of the temporary storage concept in the transport network in a supply chain perspective. 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, to the supply chain, and internal demands. The supply chain internal demands can be illustrated with scheduling of the transportation and the delivery time by extended use of just-in-time delivery. The supply chain external demand comes both from the local environment (risks from criminal activities etc.) and authorities (laws and regulations regarding transportation etc.). This means that risks and uncertainties emerge from both internal and external factors in the supply chain. For internal reasons terminal-close temporary storage places reduce uncertainty by making it smoother to schedule all delivery according to demands and needs in the receiving terminal. This also reduces the supplier upstream risk. The temporary storage function will act as supply chain disturbance neutralizer, thereby reducing risks and uncertainty within the supply chain. The external

authorities' demand on temporary storage will induce regulations regarding working hours, employee safety, refuelling, customs passage, etc.

The supply chain external environmental threat will affect the temporary storage differently than the other two main reasons for its existence. The environment surrounding the temporary storage and the supply pipeline can increase both the risks and the uncertainty in the supply chain. On the impact or consequence side of the risk there are basically three different outcomes, goods delayed, destroyed or missing. On the cause side there still are deliberate and unintentional reasons behind the consequence. The most uncertainty-generating consequence is goods missing. The missing goods can just due to a process failure or mistake be misplaced and will show up in another place than expected, or they can be stolen. The business impact will generally be higher if the goods are stolen or destroyed, than if they just are delayed. But due to penalty fees between supplier and buyer the impact can be just as serious for a delay as with a theft. As described above, the opportunity for a crime, together with a motivated perpetrator, is needed for a crime to occur. Therefore it is necessary to reduce crime opportunity in the temporary storage area in order to reduce the total risk, linked to the transportation.

This paper attempts to enlighten the role of the temporary storage concept in a supply chain perspective and its risk and uncertainty reducing abilities. The supply chain needs the temporary storage, as it is vital for the overall performance of the chain, when it comes to 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 the temporary storage will offer a crime opportunity which needs to be reduced, to achieve lower total supply chain risk and uncertainty.

4.6. Study 5: Statements about antagonistic gateways

The purpose of the survey is to verify the deductive conclusions in this thesis, formed and presented in chapter 2. A survey was conducted whereby the respondents were asked to provide their thoughts relative to 20 statements. The respondents could choose one of the following four answers: agreeing "strongly", "weakly" or "not at all" with the statement, the fourth answer was "no opinion". First, ten statements were formed by the researcher and then 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 statement document is found in appendix 2 in this thesis. 30 companies and organizations provided responses during November 2006. The participating organisations are among those presented in appendix 1. 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 as security officers, claims adjusters and criminal experts. 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 agreed that the survey was a representative view of the problem of antagonistic gateways within the transport network. The two groups also agreed that the combined conclusions, drawn from the 20 statements, were valid for the business. Some statements are more addressing attitudes; therefore the answers from the survey must be used with moderation.

This thesis uses methodology triangulation (Mangan et al., 2004). In that perspective this survey shall be seen as one corner-stone in the validation of this thesis. Some of the statements are directly aimed toward different theories from criminology, which were used in chapter 2. The purpose is to verify the need for inducing them into the scientific field of logistics. These are combined with the statements that were used as Bayes' theorem in verifying the official criminal statistics presented in chapter 1. Other statements address which risk management approach is needed in order to successfully prevent the usage of antagonistic gateways. All statements with answers and linked issues in this thesis are presented in table 10 below.

Statement:	Addresses issue:	Outcome:
1: The perpetrators endeavour to exploit the weakest link or spot, when using antagonistic gateways to either add or remove goods.	<ul style="list-style-type: none"> – Situation crime prevention – Crime displacement – Professional vs. opportunistic thief 	Strongly: 28 Weakly: 2 Not at all: 0 No opinion: 0
2: The problem with cargo theft is increasing within the transport network.	<ul style="list-style-type: none"> – Criminal statistics 	Strongly: 16 Weakly: 6 Not at all: 3 No opinion: 5
3: The transport network is very predictable, depending on the flow of resources.	<ul style="list-style-type: none"> – Routine activity perspective 	Strongly: 24 Weakly: 4 Not at all: No opinion: 2
4: The majority of the perpetrators of cargo theft are locally based, relative to where attacks occur.	<ul style="list-style-type: none"> – Routine activity perspective – Crime displacement – 	Strongly: 2 Weakly: 15 Not at all: 4 No opinion: 9
5: The fear of terrorist attacks against the transport network is the prime driver for increasing security.	<ul style="list-style-type: none"> – Risk management approach 	Strongly: 2 Weakly: 9 Not at all: 17 No opinion: 2
6: The problem with smuggling is increasing within the transport network.	<ul style="list-style-type: none"> – Inbound antagonistic gateway 	Strongly: 11 Weakly: 7 Not at all: 3 No opinion: 9
7: More use of secure parking spaces both between and close to receiver terminals could reduce the risk of theft during transportation.	<ul style="list-style-type: none"> – Situation crime prevention – Crime displacement – Routine activity perspective 	Strongly: 24 Weakly: 3 Not at all: 2 No opinion: 1
8: The major portion of economic risk with a transport is subsumed by the consignor.	<ul style="list-style-type: none"> – Risk management – Cost consequence 	Strongly: 7 Weakly: 8 Not at all: 10 No opinion: 5
9: More inspections of shipments are needed to reduce the problem of smuggling goods.	<ul style="list-style-type: none"> – Inbound antagonistic gateway 	Strongly: 21 Weakly: 2 Not at all: 3 No opinion: 4

10: The perpetrator's context (economical or political) is the key issue to understanding what the target is and how to prevent the potential incident.	<ul style="list-style-type: none"> – Situation crime prevention – Crime displacement – Risk management approach 	<p>Strongly: 19 Weakly: 7 Not at all: 2 No opinion: 2</p>
11: The increased cost for transport security will be paid by the end user.	<ul style="list-style-type: none"> – Cost consequence 	<p>Strongly: 25 Weakly: 5 Not at all: 0 No opinion: 0</p>
12: Better employee awareness against theft and smuggling within the transport network will lead to fewer incidents.	<ul style="list-style-type: none"> – Situation crime prevention – Crime displacement 	<p>Strongly: 24 Weakly: 5 Not at all: 1 No opinion: 0</p>
13: Security is also a quality aspect on the transportation.	<ul style="list-style-type: none"> – Risk management approach – Situation crime prevention 	<p>Strongly: 30 Weakly: 0 Not at all: 0 No opinion: 0</p>
14: EU regulations will enhance the transport security level within the EU.	<ul style="list-style-type: none"> – Risk management approach – Situation crime prevention 	<p>Strongly: 16 Weakly: 7 Not at all: 2 No opinion: 5</p>
15: Network-based electronic surveillance is the future of security equipment.	<ul style="list-style-type: none"> – Situation crime prevention 	<p>Strongly: 17 Weakly: 11 Not at all: 1 No opinion: 1</p>
16: Counterfeited products are difficult to distinguish from legal products.	<ul style="list-style-type: none"> – Inbound antagonistic gateway 	<p>Strongly: 17 Weakly: 5 Not at all: 0 No opinion: 8</p>
17: In the majority of cargo theft incidents goods are stolen to a small market value (up to 30,000 SEK).	<ul style="list-style-type: none"> – Situation crime prevention – Crime displacement – Routine activity perspective – Risk management approach 	<p>Strongly: 20 Weakly: 4 Not at all: 1 No opinion: 5</p>
18: The willingness to report theft incidents has declined during the recent years.	<ul style="list-style-type: none"> – Criminal statistics 	<p>Strongly: 8 Weakly: 7 Not at all: 5 No opinion: 10</p>
19: The insider problem is overrated.	<ul style="list-style-type: none"> – Internal or external theft 	<p>Strongly: 3 Weakly: 3 Not at all: 23 No opinion: 1</p>
20: Successful security also solves safety problems in transportation.	<ul style="list-style-type: none"> – Risk management approach 	<p>Strongly: 21 Weakly: 7 Not at all: 1 No opinion: 1</p>

Table 10: Statements, answers and addressed issues in study 5

The outcome from the statement survey indicates the following:

The perpetrators are generally believed to open an antagonistic gateway, where the perceived risk is as low as possible. The perpetrators also have adaptability to the normal movement and operations within the transport network. The mobility of the perpetrators is believed in general terms not to be confined to being local. This is combined with the belief that most cargo theft incidents target goods to a fairly low market value. Statement number 7 points out a belief of the business, that secure parking spaces between terminals will have a theft preventive impact on road transports. The amount of hidden statistics within the official crime statistics has presumably increased, while the actual incidents are also believed to have increased.

The problem with the inbound antagonistic gateway is more uncertain than the problem with theft (outbound antagonistic gateway). The survey shows that the problem may have increased in extent. This shall be compared with that the survey clearly indicates that more inspection of shipment needs to be executed to prevent the smuggling. If the sought-after goods are counterfeited products, then the survey expresses a disbelief in the inspector's ability to separate legal products from fake ones. The survey also indicates that the two different risk management approaches presented in this thesis are both needed as preventive methods.

5. Conclusions

This chapter contains the main conclusions of this thesis.

5.1. *Theoretical conclusions*

There are basically two types of illegal and antagonistic threats to logistics, theft/sabotage and smuggling. The theft/sabotage problem is directly aimed towards the logistics activities, while smuggling abuses the logistics system for illegal purposes. The reasons behind these problems can vary from case to case, as can the different countermeasures to prevent these problems from occurring.

This thesis addresses the problem with illegal products entering or legal ones exiting the legal transport network. Theft (exiting) and smuggling (entering) can be seen as illegal and antagonistic business processes that are autonomous or semiautonomous and managed by perpetrators, who act from a rational choice perspective. When a product changes from the legal side to the illegal side or vice versa, it uses a gateway or cross-over point. This gateway is chosen or created to minimize the risk of discovery, but also with regard to normal business constraints like cost, time, reliability etc.

To achieve a high overall supply chain performance all processes and activities need to be scheduled and managed, in order to obtain both cost efficiency and short lead-times. In the transport network this is realized by the extended use of time-windows. These windows are scheduled after 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 all actors involved, including the potential perpetrator. This predictability plays an important role in all potential crimes within the network. The need from the supply chain for a scheduling of all transportation 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 both 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. Crime opportunities in the transport network can also be seen as antagonistic and informal inbound and outbound gateways, where an antagonistic inbound gateway represents smuggling and the antagonistic outbound gateway represents theft. Sabotage is an antagonistic outbound gateway without removal of the goods.

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 that the crime brings and the troubles and risks it results in. The creation and usage of antagonistic gateways is therefore also a subject for a benefit/trouble-risk decision process from the potential perpetrator's side. Transportation security therefore aims to alter the outcome from the potential perpetrator's decision process regarding the usage of an antagonistic gateway.

The theory of crime displacement states that rationally thinking perpetrators with crime mobility will alter their criminal behaviour in response to crime prevention efforts (Lab, 2000). This means that within the potential perpetrator's capability, he will try to find a different antagonistic gateway to exploit. This risk for antagonistic gateways can in a supply chain risk context be considered a part of the environmental risk. The environment is in this case 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 are becoming more professional, they will also be able to utilize the weak spots in the transport network within their mobility and ability. The securing of the transport network can be called transport pipeline security.

The perpetrator’s decision process is the key issue to understand the usage of antagonistic gateways in the transport network. This means that a contextual risk management approach is better to use when preventing the usage of antagonistic gateways. In other words, the countermeasures need to be based on an understanding of this decision process, the antagonistic dynamics of potential perpetrators. The difference in perpetrator context is vital for applying the right type of transport pipeline security countermeasures. Security against these types of antagonistic threats in the transport network aims to alter the contextual perception of the network, thereby reducing the problem with antagonistic gateways. In figure 17, the three research questions in this thesis are presented in relation to transport pipeline security, antagonistic gateways and the transport network.

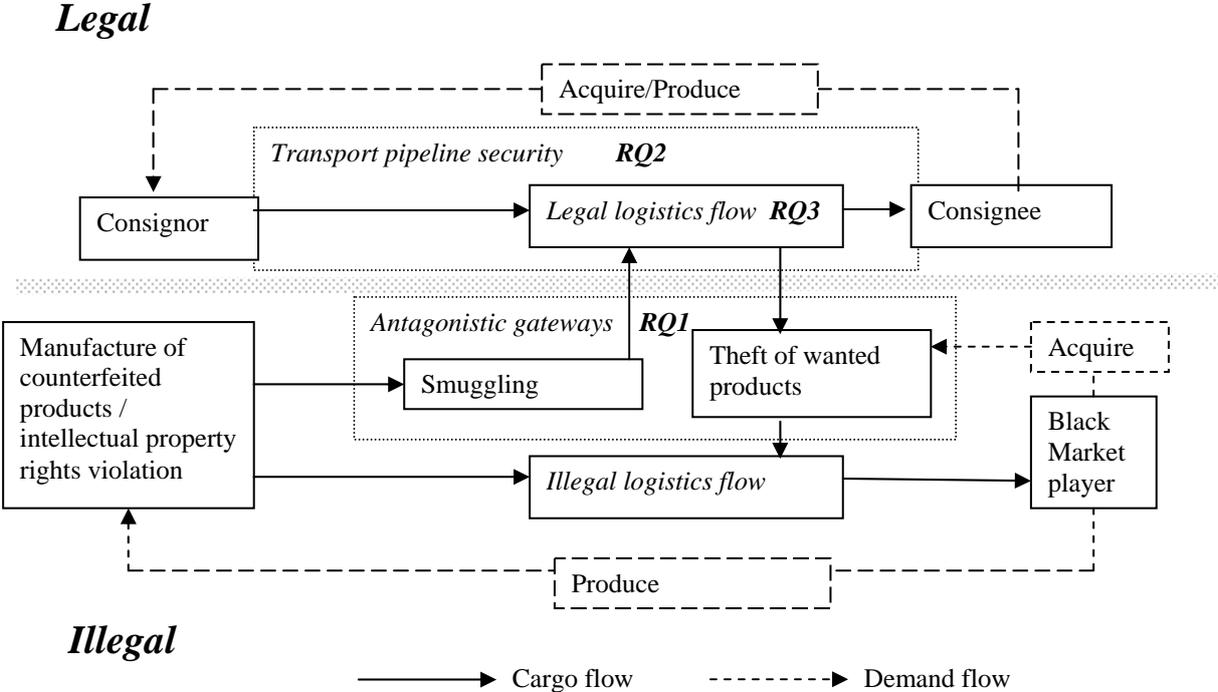


Figure 17: Antagonistic gateways in the transport network in a supply chain perspective

5.2. Generalisation

RQ 1 What are the characteristics of the antagonistic gateways between legal and illegal logistics systems?

The answer to this question is found mainly in the frame of reference, with the description and demarcation for the two logistics systems, presented in paper B. An antagonistic gateway needs two things in order to become opened, namely an opportunity and a motivated perpetrator. This shall be compared with the three elements of crime, namely motivated perpetrator, suitable object and lack of capable guardian. This implies that a crime opportunity represents the unique combination of object and guardian for each moment. Therefore an antagonistic gateway is each and every unique combination of target and guardian for each moment. This gateway is then subject to the perpetrator's decision process, if it is to become used or not. The potential usage can be prevented by transport pipeline security countermeasures implemented by the actors in the transport network. It aims to reduce crime opportunities by increasing the presence (or perceived presence) of a guardian. Transport pipeline 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 implemented both in terminals and in the resources moving between them.

RQ 2 How can these gateways be prevented?

The prevention of the usage of the antagonistic gateway is based on situation crime prevention theory. The situation crime prevention comprises four basic parts or steps, namely increasing perceived effort, increasing perceived risk, reducing anticipated reward and inducing guilt or shame. Common for all these four parts is that the target to perceive these preventive actions is the potential perpetrator.

The four basic parts in situation crime prevention theory must be adapted to suit the needs of the transport network. The available resources that a Logistics Service Provider (LSP) can utilize are the employees, technologies, routines and the design of the network with respect to terminals, cargo carriers and route choice. The network design will be addressed in RQ3. To utilize the employees, different routines and technologies in a situation crime prevention context will prevent the usage of antagonistic gateway by limiting the accessible crime opportunities. All these countermeasures need to be carefully elaborated, so the effectiveness of the network will be greatly unaffected. The aim of transport pipeline security is to protect the flow of material, primarily from antagonism during the complete transport from consignor to consignee but also other types of threats, and still accomplish an effective business, by utilizing the right mixture of technologies and human involvement.

The basics of transport pipeline security should be to protect fixed assets like terminals, warehouses, harbours, airports and manufacturing plants. The next step is to enlarge the security thinking out of the gates from the fixed assets to the links between the fixed assets. The general idea is that it would be both too hard and too risky to either add goods to or remove goods from the shipment. Transport pipeline security also needs to incorporate all stakeholders in the transport network to avoid weak spots as far as possible.

RQ 3 What are the effects on transport network design of the existence of antagonistic gateways?

The design of the transport network is conducted primarily 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. The 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. The second constraint is the cost for the network and that economical impact from usage of an antagonistic gateway is one component of the total cost. This means that if the economical impact from antagonistic gateways becomes too large (relative to other costs for that particular stakeholder) it will affect network design more and more. The eighth statement in the fifth study indicates that the different stakeholders do not agree about who subsumes the largest part of the economical risk with a transport. This answer clearly shows the complexity and the difficulty surrounding the existence of antagonistic gateways.

The changes in network design can be more rigid scheduling and shipments, forcing the network into using other routes and also increasing the usage of preventive measures to reduce the problem of antagonistic gateways. The effects that such gateways will have on transport network design will always be addressed through a cost-benefit analysis. The conclusion from paper A together with the conclusions from study 3 and paper C provides the crucial issue, i.e. the perpetrators' decision process, which depends on perceived risk and difficulty to fulfil that usage of the gateway in relationship to the expected benefit for it. There will always be points or links in the network that will have the weakest defence against these gateways. By changing the network setup these spots will also change.

6. Further research

This thesis takes a top-down perspective on the problem with antagonistic gateways in a transport network. This means basically that the logistics business has been simplified to be made up of a transport network in the form of a system, with a related illegal logistics system, where both are parts of different supply chains. In reality several actors and companies do business within the transport network. Each different actor or stakeholder can address the problem with antagonistic gateways differently and thereby affect the whole system's preventive actions. This difference was evident in study 5 even if the different stakeholders agreed about the general view in almost all of the 20 statements used in that study. This problem will be addressed in future work.

According to the theory of situational crime prevention, there are four basic ways to prevent crime. The three first parts are most commonly used by the transport network, but the fourth one is not being used to prevent crimes. The fourth principle is to induce guilt or shame into the potential perpetrator. This preventive method may be the most effective to prevent employee usage of antagonistic gateways. This principle aims to appeal to people's moral and make it easy for them to do the right thing, then excuses will be more difficult to use. The outcome from the twelfth statement in study 5 indicates that the stakeholders in the transport network believe that better awareness among their employees will reduce the risk for antagonistic gateways within the company's responsibility. How big the awareness is among employees today, and how that awareness can be increased will be addressed in future research.

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?

The eighteenth statement in study 5 addresses the problem with insiders, who commit crime within the organisation to which they belong. An inside position or inside information about a certain shipment or transport is useful to have for a potential perpetrator. The literature has different opinions about the seriousness in the fear about insiders. 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 shall be compared with that 23 out of 30 organisations, in study 5, 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 are as serious as the stakeholders claim in study 5, how can preventive measures be induced into the transport network, which address the problem with internal thieves?

The eighth statement in study 5 is where the answers are the most disparate. It addresses the economical impact from an incident that damages the goods or where they become stolen. Why is there a disagreement about how the economical impact is subsumed by the different stakeholders in a transport?

7. References

- Almay, T. (2006), "Seeing the risk through the trees". *Security management*, September 2006, pp.101-112, ASIS international.
- Arbnor, I. and Bjerke, B. (1997), *Methodology for creating business knowledge*, SAGE Publications, California.
- Barr, R. and Pease, K. (1990), "Crime placement, displacement and deflection". In Tonry, M and Morris, N (ed.), *Crime and justice*, Vol. 12. Chicago: University of Chicago press.
- Barth, S. and White, M. D. (1998), "Hazardous cargo". *World Trade*, November 1998, pp. 29,
- Beck, A. (2002), "Automatic product identification & shrinkage: Scoping the potential". ECR, Brussels.
- Bodman, P. and Maultby, C. (1997), "Crime, punishment and deterrence in Australia". *International journal of social economics*, Vol 24. pp 884-901.
- Brindley, C. (2005), *Supply chain risk*. Ashgate Publishing England
- Burnett, J. (2002), *Dangerous waters*. Penguin Putnam Inc.
- Cavinato, J. (2004), "Supply chain logistics risks: From the back room to the board room". *International journal of physical distribution & logistics management*, Vol. 34 No. 5, pp. 383-387.
- Chapman, P., Christopher, M., Juttner, U. and Peck, H. (2002), "Identifying and Managing Supply Chain Vulnerability". *Logistics & transport focus*, Vol.4, No. 4, pp. 59-64.
- Christopher, M. (1992), *Logistics and Supply Chain Management*, 1st ed., Financial Times/Pitman, London.
- Christopher, M (1998) *Logistics and Supply Chain Management*, Prentice Hall London
- Christopher, M. and Lee, H. (2004), "Mitigating supply chain risk through improved confidence". *International journal of physical distribution and logistics management*, Vol. 34 No. 5, pp. 388-96.
- Christopher, M. and Peck H. (2004), "Building the resilient supply chain". *International journal of logistics management*, Vol. 15 No. 2, pp. 1-13.
- Clarke, R. V. and Cornish, D. (1985), "Modelling offenders decisions: A framework for policy and research". In Tonry, M and Morris, N (ed.), *Crime and justice*, Vol. 4. Chicago: University of Chicago press.
- Clarke, R. V. (1992), *Situational crime prevention: Successful case studies*. Harrow and Heston, New York.

Clarke, R. V. and Cornish, D. (1990), "Crime specialization. Crime displacement and rational choice". In: Wegener, H. (eds), *Criminal behaviour and justice system*. New York: Springer-Verlag.

Clarke, R. V. (1995), "Situational crime prevention". In Tonry, M. and Farrington, D.P. (eds), *Building a safer society: strategic approaches to crime prevention*. Chicago: University of Chicago press.

Clarke, R. V. and Homel, R. (1997), "A revised classification of situational crime prevention techniques". In Lab, S. P. (ed.) *Crime prevention at a crossroads*. Andersson Publishing Co Cincinnati US.

Clarke, R. V. and Cornish, D. (2003), "Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention". *Crime prevention studies*, vol. 16, pp.41-96.

Closs, D. and McGarrell, E. (2004), "Enhancing Security Throughout the Supply Chain". IBM Centre for the business of government.

Clutterbuck, R. (1987), *Kidnap, hijack and extortion*. Basingstoke Macmillan, London

Cohen, L. E. and Felson, M. (1979), "Social change and crime rate trends: A routine activity approach". *American sociological review*, Vol. 44, pp. 588-608.

EC (2003), "Freight Transport Security". *Consultation paper*, European Commission, Brussels.

Crawford, A. (1998), *Crime prevention and community safety: Politics, policies and practice*. Longman London.

Dillén, J. and Ekwall, D. (2006), "Brott mot yrkestrafiken". *Transek 2006:10* (in Swedish).

Dubois, A. and Gadde, L.-E. (2002), "Systematic combining: an abductive approach to case research". *Journal of business research*, Vol 55, No 7, pp.553-560.

ECMT (2001 - a), *Theft of goods and goods vehicles*. CEMT/CM (2001)19, Lissabon.

ECMT (2001 - b), *Improving security for road freight vehicles*. Paris: OECD Publication Service

ECMT (2002), "Crime in road freight transport". OECD Publication Service, Paris.

Ekwall, D. (2006), "Cargo theft in supply chains: Crime displacement in the transport network".

Felson, M. and Clarke, R.V. (1998), "Opportunity makes the thief: Practical Theory for crime prevention". Home office police and reducing crime unit: London

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

- Findlay, M (1999) *The globalisation of crime*. Cambridge University Press. New York
- Gips, M. (2006), "Cargo security getting some respect". *Security management*, July 2006, pp.28, ASIS international.
- Giunipero, L. and Eltantawy, R. (2004), "Securing the upstream supply chain: a risk management approach". *International journal of physical distribution & logistics management*, Vol. 34, No. 9, pp. 698-713
- Hellevik, O. (1984), "Forskningsmetoder i sociologi och statsvetenskap". Natur och kultur, Stockholm (In Swedish).
- Helliar, C. and Lonie, A. and Power, D. and Sinclair, D. (2001), "Attitudes of UK Managers to Risk and Uncertainty". *The Institute of chartered accountants of scotland*, Bell and Bain Ltd, Glasgow.
- Hesseling, R. (1994), "Displacement: A review of the empirical literature". In Clarke, R. (ed.) *Crime prevention studies*, Vol 3, 197-230. Monsey, NY: Criminal Justice Press.
- Holme- Solvang (1997), *Forskningsmetodik*. Lund: Studentlitteratur
- Horney, J. and Marshall, I. H. (1992), "Risk perceptions among serious offenders: the role crime and punishment". *Criminology*, Vol. 30, No. 4, pp. 575-594.
- IACC, (2005), *White paper, The negative consequences of international intellectual property theft* . Washington.
- Johns, T. and Hayes, R. (2003), "Behind the fence: Buying and selling stolen merchandise". *Security journal*, Vol. 16: No. 4, Perpetuity Press.
- Juttner, U. (2005), "Supply chain risk management: Understanding the business requirements from a practitioner perspective". *The international journal of logistics management*, Vol. 16 No. 1, pp. 120 – 141.
- Kelleher, G. and El-Rhalibi, A. and Arshad, F. (2003), "Scheduling for intermodal transport". *Logistics information management*, Vol. 16, No. 5, pp. 363-372.
- Kallis, and Vanier, (1985), op cit, Hayes, R. (1997) "Shop Theft: An Analysis of Apprehended Shoplifters", *Security journal*, Vol. 7, pp. 11-14
- Klemke, L. (1992 - A), "The Sociology of Shoplifting: Boosters and Snitches Today", New York: Praeger.
- Klemke (1992 - B) op cit.; Shapland, J. (1995) "Preventing Retail Sector Crimes", in M. Tonry and D. Farrington (Ed.) *Building a safer society: strategic approaches to crime prevention*, Chicago: The University of Chicago Press.

- Klaus, P., Henning, H., Muller-Steinfahrt, U. and Stein, A. (1993), "The promise of interdisciplinary research in logistics". in Masters, J.M. (Ed.), *Proceedings of the twenty-second annual transportation and logistics educators conference*, pp. 161-87.
- Kekäle, T. (2001), "Construction and triangulation: weaponry for attempts to create and test theory". *Management decision*. Vol. 39, No. 7, pp. 556-563.
- Lab S. P. (2000), *Crime prevention: Approaches, practices and evaluations*. Fourth edition. Andersson Publishing Co, Cincinnati US.
- Lalwani, C.S and Disney, S. M. and Naim, M. M. (2006), "On assessing the sensitivity to uncertainty in distribution network design". *International journal of physical distribution & logistics management*, Vol. 36. No. 1, pp. 5-21.
- Lambert, D. and Stock, J. (1993) *Strategic logistics management*. Richard D Irwin Inc, US.
- Lambert, D. and Stock, J. and Ellram, L. (1998), *Fundamentals of Logistics Management*, International ed., McGraw-Hill Higher Education, London.
- Larmour, P. and Wolanin, N. (2001), *Corruption and anti-corruption*. Canberra: Asia Pacific Press.
- Lee, L. and Whang, S. (2003), "Higher supply chain security with lower cost: Lessons from total quality management". *International journal of production economics*, 96 pp. 289–300.
- Lin, F. and Shaw, M.J. (1998), "Reengineering the order fulfillment process in supply chain networks". *The International journal of flexible manufacturing systems*, Vol. 10, No. 3, pp. 197-229.
- Lumsden, K. (2006), *Logistikens grunder*. Studentlitteratur, Lund (in Swedish)
- Mankin, N. G. (1997), *Principles of microeconomics*. The Dryden Press, Fort Worth Texas.
- Manunta, G. (1999), "What is security?". *Security journal*, Vol. 12, No. 3, pp 57-66, Perpetuity Press.
- Manunta, G. (2002), "Risk and security: Are they compatible concepts?". *Security journal*, Vol. 15, No. 2, pp 43-55, Perpetuity Press.
- Mishler, E. (1986), *Research Interviewing*. First Harvard Press, Boston.
- Muir, J. (1996), "Theft at work". *Work Study*; Vol. 45.
- Napoleoni, L (2004) *Terror inc*. Penguin books ltd.
- Naylor, R (2004), *Wages of crime*. Cornell University Press. Ithaca.
- NCO (2006), "Att säkra godsflöden". *Arbetsrapport NCO 2006:2*, Räddningsverket (in Swedish)

- Nilsson, F. (2004), "Simplicity vs Complexity in the Logistics Discipline – A Paradigmatic Discourse". *NOFOMA*, Linköping.
- Nilsson, F. (2006), "Logistics management in practice – towards theories of complex logistics". *The International journal of logistics management*, Vol. 17, No. 1, pp. 38-54.
- Nowotny, H. and Scott, P. and Gibbons, M. (2002), *Re-Thinking Science*. Blackwell Publishers ltd, UK.
- Popper, K. (1959), *The logic of scientific discovery*. Routledge London.
- Prater, E. and Biehl, M. and Smith, M. (2001), "International supply chain agility, Tradeoff between flexibility and uncertainty". *International journal of operations & production management*, Vol. 21 No. 5/6, pp. 823-839.
- Purtell, D. and Rice, J. B. (2006), "Assessing cargo supply risk". *Security management*, November, 2006, pp.78-87, ASIS international.
- Repetto, T. A. (1974), *Residential crime*. Cambridge.
- Repetto T. A. (1976), "Crime prevention and the displacement phenomenon". *Crime and delinquency*, Vol. 22, pp. 166-177.
- Samaranayake, P. (2005), "A conceptual framework for supply chain management: a structural integration". *Supply chain management: an international journal*, Vol. 10, No 1, pp 47–59.
- Sarnecki, J. (2003), *Introduktion till kriminologi*. Studentlitteratur, Lund (in swedish)
- Sheffi, Y. (2001), "Supply chain management under the threat of international terrorism". *International journal of logistics management*, Vol. 12, No. 2, pp. 1-11.
- Speed, M. (2003), "Reducing employee dishonesty: In search of the right strategy". *Security journal*, Vol. 16, No. 2, pp 31-48, Perpetuity Press.
- Stefansson, G. (2004), *Collaborative Logistics Management*. Chalmers, Gothenburg.
- Stock, J. R. (1997), "Applying theories from other disciplines to logistics". *International journal of physical distribution & logistics management*, Vol. 27, No. 9, pp. 515-539.
- Sutherland and Cessey and Luckenbill (1992), *Principles of Criminology, 5th Edition*. Kenner Books, IL, US.
- Svensson, G. (2002), "A conceptual framework of vulnerability in firms' inbound and outbound logistics flows", *International journal of physical distribution & logistics management*, Vol. 32, No. 2, pp. 110-34.
- Sweet, K. (2006), *Transportation and Cargo security*. Pearson Prentice Hall, New Jersey.

TRA (2006), Transport Research Arena Europe, Greener, safer, and smarter road transport for Europe, Göteborg 12 - 15 June 2006, <http://www.traconference.com/273.aspx>

Tryon, G. and Kleiner, B. (1997), "How to investigate alleged employee theft properly". *Managerial auditing journal*, Vol. 12, MCB University Press.

Tyska, L.A. and Fennelly, L.J. (1983), *Controlling cargo theft*. Woburn: Butterworth Publishers, Boston.

Tyska, L.A. and Fennelly L.J. (2001), *Cargo theft prevention*. ASIS, US.

Waidringer, J. (2001), *Complexity in Transportation and Logistics Systems*. Chalmers, Gothenburg.

Wandel, S. and Ruijgrok, C. (1995), "Information technologies for the development of transport and logistics". *ATAS Bulletin information for development*, United Nations New York.

Wang, J. and Roush, M. (2000), *What every engineer should know about risk engineering and management*. Marcel Dekker inc. New York.

White, D. (1995), "Application of systems thinking to risk management: a review of the literature". *Management decision*, Vol. 33, No. 10, pp. 35-45.

Wilson, B. (1990), *Systems: concepts, methodologies and applications*. John Wiley & Sons, New York.

Winterburn, R. (2005), "A review of 2004 freight crime using TAPA EMEA IIS data". *A presentation in Brussels* – February.

Yin, R. (1989), *Case study research. Design and method*. Sage publications Thousand Oaks California.

Zsidisin, G. and Panelli, A. and Upton, R. (2000), "Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study". *Supply chain management: an international journal*, Vol. 5, No. 4, pp. 187-198.

Weaver, F. and Carroll, J. (1985), "Crime Perceptions in a Natural Setting by Expert and Novice Shoplifters", *Social psychology quarterly*, Vol. 48, No. 4, pp. 139-359,

Yin, R. K. (1994), *Case study research: design and methods*. Sage, Thousand Oaks, CA.

WEB:

TAPA, Technology Assets Protection Association, <http://www.tapaemea.com/engl/index.html>

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

EC-web, European Commission: Counterfeit and piracy, Introduction, http://europa.eu.int/comm/taxation_customs/customs/customs_controls/counterfeit_piracy/index_en.htm (printed 2005-03-24)

Appendix 1 – 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
DFDS Transportation
DHL Express
DHL Solutions
Frigoscandia Distribution
Green Cargo
Pan Nordic Logistics
SAS Cargo
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
YourSec

Authorities

National Criminal Investigation Department
Swedish Customs
Swedish Police
Swedish Coast Guard

Appendix 2 – Questionnaire for the statements about antagonistic gateways in the transport network

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

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

2: The problem with cargo theft is increasing within the transport network.

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

3: The transport network is very predictable depending on the flow of resources.

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

4: The majority of the perpetrators of cargo theft are locally based, relative to where attacks occur.

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

5: The fear of terrorist attacks against the transport network is the prime driver for increasing security.

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

6: The problem with smuggling is increasing within the transport network.

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

7: More use of secure parking spaces both between and close to receiver terminals could reduce the risk of theft during transportation.

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

8: The major portion of economic risk with a transport is subsumed by the consignor.

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

9: More inspections of shipments are needed to reduce the problem of smuggling goods.

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

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

Agree: *Strongly* *Weakly* *Not at all* *No opinion*

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

Agree: Strongly Weakly Not at all No opinion

12: Better employee awareness against theft and smuggling within the transport network will lead to fewer incidents.

Agree: Strongly Weakly Not at all No opinion

13: Security is also a quality aspect on transportation.

Agree: Strongly Weakly Not at all No opinion

14: EU regulations will enhance the transport security level within the EU.

Agree: Strongly Weakly Not at all No opinion

15: Network-based electronic surveillance is the future of security equipment.

Agree: Strongly Weakly Not at all No opinion

16: Counterfeited products are difficult to distinguish from legal products.

Agree: Strongly Weakly Not at all No opinion

17: In the majority of cargo theft incidents goods are stolen to a small market value (up to 30,000 SEK).

Agree: Strongly Weakly Not at all No opinion

18: The willingness to report theft incidents has declined during the recent years.

Agree: Strongly Weakly Not at all No opinion

19: The insider problem is overrated.

Agree: Strongly Weakly Not at all No opinion

20: Successful security also solves safety problems in transportation.

Agree: Strongly Weakly Not at all No opinion

Paper A

Cargo theft from supply chains: Crime displacement in logistics

Daniel Ekwall

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

Abstract

Purpose – To analyze why cargo theft continues to occur in the transport network despite all countermeasures induced by the business. Cargo theft is a significant problem to today's supply chain performance. Although some countermeasures have been successfully employed, this problem continues to plague transport networks.

Design/methodology/approach – Forming a hypothesis through a logical deductive process. The hypothesis is based on several different theories and validated with the use of a methodology triangulation. This hypothesis is then validated with several interviews and statistics from independent sources.

Findings. - The theft risk arises from different theft opportunities that will always be present in a transport network. 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. The theory of crime displacement in the transport network explains why the absolute reduction is hard to achieve if an integrated systems approach is not used to secure the effectiveness of countermeasures for the whole supply chain.

Research limitations/implications –This research is limited by the lack the reliability of the information about criminal activities against logistics. The normal secondary sources like official crime statistics are at its best untrustworthy but more likely filled with large parts of hidden statistics. Therefore this paper is based on a theoretical deduction, several interviews and statistics from independent sources.

Practical implications – The result is a direct correlation between preventive countermeasures, the potential offender's reactions and the need for an integrated system approach in order to reduce the cargo theft problem.

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

Keywords: Supply Chain Management, Cargo Theft, Crime Prevention, Transport Network, Crime Displacement, Supply Chain Risk Management

Paper type: Research paper

Background

From the beginning of mankind there has always been some form of trade. This trade usually required some type of transport and most likely involved unwanted risk from the goods being stolen or sabotaged. Historically, even states have sponsored and exploited systematic theft of cargo from ships by using privateers. Today there is a significant problem with the theft of cargo worldwide. It is estimated that theft represents losses of at least US \$ 10 billions per year in the United States and US \$ 30 billion worldwide (Barth et al., 1998). These figures are calculated extraordinarily conservatively due to that most cargo theft goes unreported and these figures reflect only the value of the items and nothing more (Barth et al., 1998). 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).

In recent years, the cargo transport process has improved mainly in the areas of logistics efficiency and documentation handling. Although, security within the cargo transport process has not been as fortunate. This deficiency changed with the World Trade Centre terror attack. The aftermath to 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. One of the many causes these disturbances in the supply chain is the problem of cargo theft. As a result, cargo theft has grown to become a substantial problem that affects all modes of transport and industry worldwide. 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. 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.

Research and method 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. For the purpose of clarity, this paper will make the assumption that all cargo is the same, irrespective of its content. This demarcation is stated to simplify research. The research question in this paper is why cargo theft within transport networks continues to be a significant problem despite the implementation of numerous countermeasures. The research method used in this paper is deductive; hence a hypothesis is developed by logical deduction from existing theories. This helps to substantiate the objectivity of this research (Popper 1959). 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). The hypothesis is then compared to the context of transport networks, from which it was developed (Popper 1959). Credibility is substantiated by using a mixture of quantitative and qualitative methods as well as several independent statistics sources,

so called methodology triangulation (Mangan et al., 2004). 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 of theoretical assumptions. To strengthen the theoretical credibility, several interviews of key personnel were conducted. All interviews were conducted in an open and descriptive manor to insure that the interviewees stated their true opinion and only to describe the problem without making any judgement about it (Mishler 1986).

Supply chain 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 at the right place (Christopher 1998). To be successful, all aspects concerning operations and information need to work together. The chain of companies that co-operate to fulfil the scope of logistics is called the supply chain. Figure 1 illustrates the total logistics system concept, from a company perspective with only one supplier and one customer.

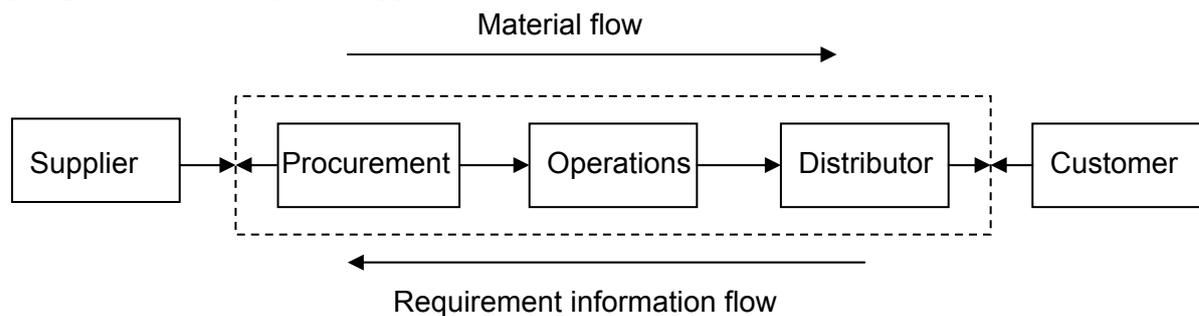


Figure 1: The total logistics system concept

The reality is far more complex. For this reason, it is better to focus on supply networks instead of supply chains. With this said, every link in a supply network is like a chain link which when put together is the basis of the term supply chain. 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 means of connecting the nodes. The transport network affects cost, throughput time, and if used smartly it can even increase the value of the product (Lambert et al., 1993). The relationship between consignor and consignee through the transport network is illustrated in figure 2.

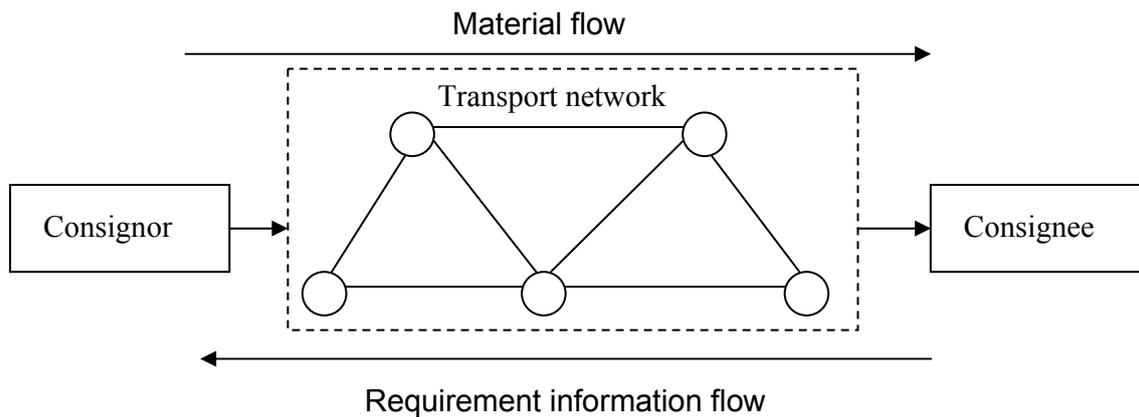


Figure 2: Transport network as a part of the supply chain

Cargo theft as a supply chain risk source in transport networks

Historically, security and vulnerability within the supply chain were largely neglected until the World Trade Centre terrorist attack. The subjects of supply chain 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. Christopher and Lee suggest that the increased vulnerability in supply chains is a result of the drive towards more efficiency which also in turns increases vulnerability from disruptions or disturbances (Christopher et al., 2004). To reduce this vulnerability companies must identify its own internal risk but also the risk that is derived from collaboration and linkage with other companies (Juttner 2005). Each company in a supply chain increases its own risk when it becomes a member of a supply chain (Finch 2004). Different risks to a supply chain can be categorized according to the source of the risk position in relationship to the supply chain itself. The source can be either internal or external to the chain (Mason-Jones et al., 1998). Juttner (2005) states that risk taking is generally perceived as an inevitable aspect of supply chain management. But, taking risks is not the same as controlling and managing risk to an acceptable level.

According to Christopher and Peck (2004), 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. 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 and supplier related problems (Zsidisin et al., 2000). Sources of environmental risks are politics, nature and social uncertainties (Juttner 2005). 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). Figure 3 illustrates the relationship and interdependency of the five sources of supply chain risk.

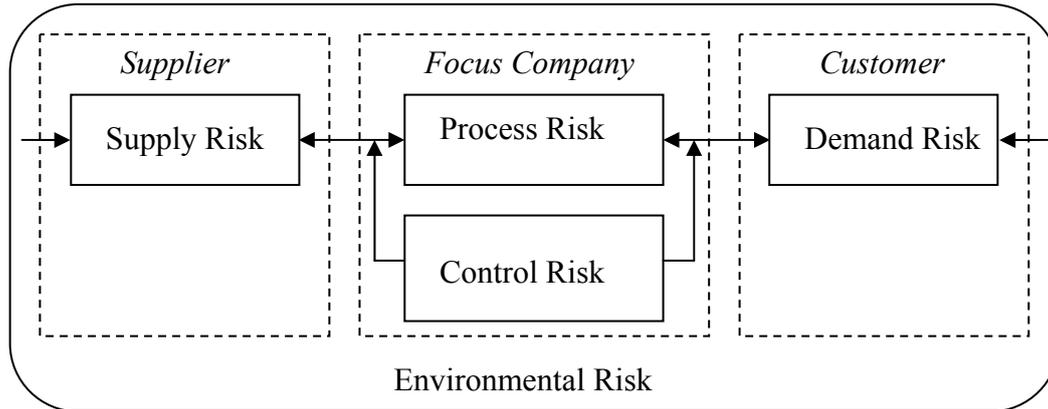


Figure 3: Sources of supply chain risks (Christopher et al., 2004)

The concept of risk combines probability and consequence for a certain event (Wang et al., 2000). Risk consequences can be subdivided into two types, namely stoppage and drainage. The impact of a stoppage is catastrophic, temporary to nature and more costly than drainage is. A stoppage is often caused by a breakdown of vital equipment, a labour strike, a terrorist attack or a legal action (Chapman et al., 2002). Drainage consequences are a loss of goods during production or transport. It affects a lesser portion of the total amount of goods or money within a supply chain and thereby receives less attention from management than a stoppage. On the other hand, if drainage has higher probability than a stoppage, the cost consequence could be similar. The risk source for a stoppage consequence is more likely to be an external or environmental risk source. Risk consequences can be either amplified or absorbed by supply chain control mechanisms such as batch sizes, inventory safety margins, decision rules and policies regarding order quantities (Juttner 2005). The stoppage effect can also be reduced by creating redundancy in the supply chain by using two or more suppliers or transport routes for each component (Sheffi 2001).

The risk for cargo theft in the transport network is, from a supply chain risk source perspective, found in the two external sources supply and demand risks. Cargo theft affects inbound and outbound logistics and the supply chain is generally more vulnerable to disruption in inbound than outbound logistics (Svensson 2002). The main consequences from a cargo theft incident is normally drainage but if the stolen amount of goods is large enough (relative to the inventory level in the supply chain), it could also have a stoppage effect (Giunipero et al., 2004). A cargo theft incident can be categorized as a transport disruption caused by either external (environmental risks) or internal (process or control risks) uncertainties affecting the transport network, thereby affecting the supply chain. Risk sources in the transport network are illustrated in figure 4.

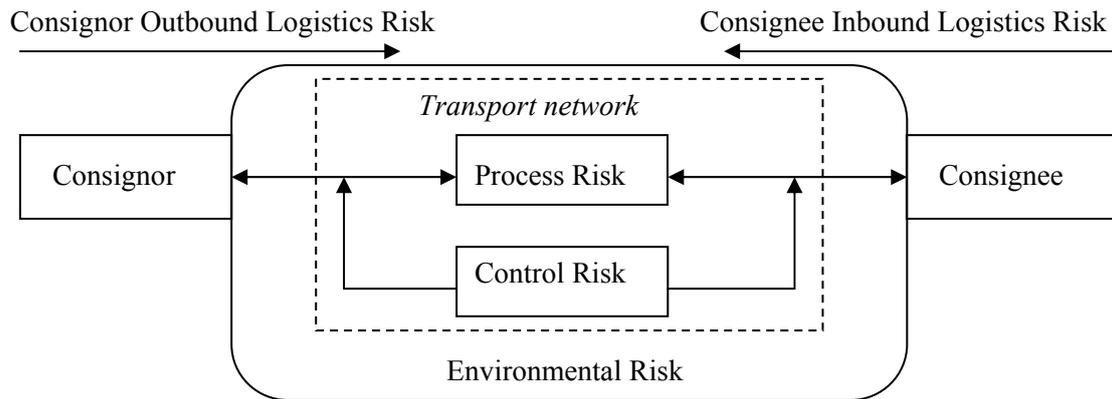


Figure 4: Sources of risk in the transport network, from a supply chain perspective

The causes for a risk can be either deliberate or unintentional. The unintentional causes are normally called process failures while the deliberate ones are antagonistic risks to the supply chain. Cargo theft is among sabotage, terrorist attack or a labour strike typical antagonistic risks and because the difference in objective they have different consequences as well. The consequence of a labour strike or a terrorist attack differs from a cargo theft incident by virtue of the perpetrators objective. Striking labours or terrorists desire public attention while cargo thieves want anonymity. The perpetrator of cargo theft is a person that has an inside or an outside relationship with the transport network and makes the choice to steal goods by using or creating an opportunity to theft. To understand the cargo theft problem in a transport network context, it is important to understand theft characteristics, countermeasures and the interaction between these components.

Theft opportunities

The hub and spoke design of a transport network is a viable configuration to achieve 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 coordinated. 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. A transport network is therefore, simultaneously predictable and unpredictable. This systematic rhythm provides theft opportunities according to Cohen and Felson's (1979) theory of routine activities perspective. This theory is a strong theoretical foundation to understand crime and opportunities for crime. The routine activities perspective argues that normal movement and local environment plays a significant role in the interaction between the potential perpetrator and the victim in a crime. Thus, when a transport network changes so does the theft opportunity.

Crime opportunity is a cornerstone in all criminal behaviour, but opportunity alone does not lead to a crime (Felson et al., 1998). Perpetrators evaluate the situation or the opportunity by using external and internal variables and then decide how they best proceed. 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.*

Altogether, these principles imply that the key issue is theft opportunity for both potential perpetrators and appropriate countermeasures. In terms of sources of supply chain risk, the issue of theft opportunity is the common deterrent in all sources of cargo theft risk. The opportunity is different in each situation and therefore needs to be reduced in each situation. This method is called situational 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. 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 et al., 1985). The rational choice theory states that an individual makes a decision on whether 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 (Repetto 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 et al., 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). 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):

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

Increase perceived risks (Clarke 1992) – If perpetrators think that they will get away with a theft, it is more likely that they will commit it. By increasing the risk for

perpetrators they are less likely to commit a theft. This can be accomplished by using surveillance systems and security personnel and by increasing employees' 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 the potential perpetrators. This can be accomplished by marking the goods with either unique numbers or a product destroying device. Good examples of this principle are the safety case used in transports of valuables and money and the inc-tags used in fashion stores.

In 1997 Clarke and Homeled add a fourth preventive principle based on rational choice theory as follows:

Inducing guilt or shame (Clarke et al., 1997) – A theft is more likely to occur if it can be excused by appeal to reasons like “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 ethnical relativity. Companies and organizations can affect this ethnical relativity by using company rules, signs and regulations that demonstrate the right moral values. When theft is seen as an additional wage benefit for the employees this preventive action has failed (Muir 1996). By appealing to people’s moral and making it easy for them to do the right thing, then excuses will be more difficult to use (Clarke et al., 1997).

Transport network theft and countermeasures

The risk for cargo theft in transport networks emerges from different theft opportunities. Therefore, to understand the cargo theft problem it is important to understand theft characteristics, countermeasures and the interaction between these components. The management approach to reduce the impact of this problem is called transport security. Transport security means the interaction between physical obstructing artefacts (locks, fences, cctv etc.) and the intervention of humans with the aim of reducing theft, sabotage and other types of illegal activities (EC 2003). 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 et al., 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 employ 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 thefts.

According to Fennelly and Tyska (1983), cargo theft situations occur when the three C’s, Confusion, Conspiracy and the Common denominator, of cargo theft is in place. These factors can best be explained with the following statement, “Lack of management control precipitates confusion, and confusion is the turned soil wherein conspiracies grow” (Tyska et al., 1983). The three C’s indicate that different settings or

configurations can increase the risk for a cargo theft incident. The three C's of cargo theft demonstrates that a potential perpetrator will use a lack of control to create or amplify a theft opportunity. The cargo theft occurs most often in trucking (Tyska et al., 1983). It is often committed by a truck driver and a warehouse employee working together. This combination clearly demonstrates where cargo theft risk is most probable, i.e. when goods are loaded and unloaded (Tyska et al., 1983). Apart from the financial loss, thefts add a feeling of uncertainty between the employer and employees, as well as between employees (Mayhew 2001).

The configuration of transport networks lead to that security measures are needed in different forms depending on the exact function and appearance of each node and link. Each part of the network can use situational crime prevention methods, but for business reasons the main focus should be to make the crime harder and riskier to commit. The three C's of cargo theft are useful in understand why one node or link is more likely to suffer from theft incidents than another, regardless of implemented countermeasures. This demonstrates that the risk for a cargo theft incident is different in each part of the transport network. Generally the highest risk for a cargo theft incident is in the node/link interface, when loading or unloading (Mayhew 2001). The rational choice theory states that a potential perpetrator evaluates different factors to establish the time, place, method and target with the highest probability of success (Lab 2000). This leads to the theory of crime displacement as a result of crime prevention.

Cargo theft 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).

Crime displacement assumes that crime is inelastic (Repetto 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 (Repetto 1976).

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

There exists 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 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 et al.,

1985). The key element in all crime is the role that opportunity plays, i.e. *if there is no opportunity there is no crime*. Based on the ten principles of theft opportunities, presented earlier in this paper and the configuration of the transport network, it is obvious that all opportunities can not be eliminated but rather they can be reduced by implying substantive preventive countermeasures. The object is to reduce crime opportunities which will lead to a change in all potential theft situations and therefore crime displacement is a valid theory (Repetto 1976).

Crime displacement can occur in several ways. Repetto (1976) uses five types of displacement – crime, target, method, place and time. Barr and Pease (1990) add another type of displacement, namely the perpetrator. Thus, 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 attractable to them than others. Furthermore, it does not explain what are 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 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 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.

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. This is crime displacement in the transport network. The key aspect to understanding

this effect is the knowledge that the potential perpetrator only respond 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*”.

Transport network expert’s interviews

To verify the theory of crime displacement were six interviews conducted with key personnel. 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 would 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.

Question 1: Describe cargo theft and preventive measures in the logistics business 10 to 20 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. The problem escalated according to the development where “an item became a box became a pallet”. This development can be described as cargo theft evolved to a professional activity from being of pilferer nature. The theft characteristics transformed from a self persuaded wage benefit to become 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 those 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 increased substantially. In the early 90’s 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.

Question 2: 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 80's 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 nowadays is 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 is demanding 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. 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. 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.

Summary from the interviews

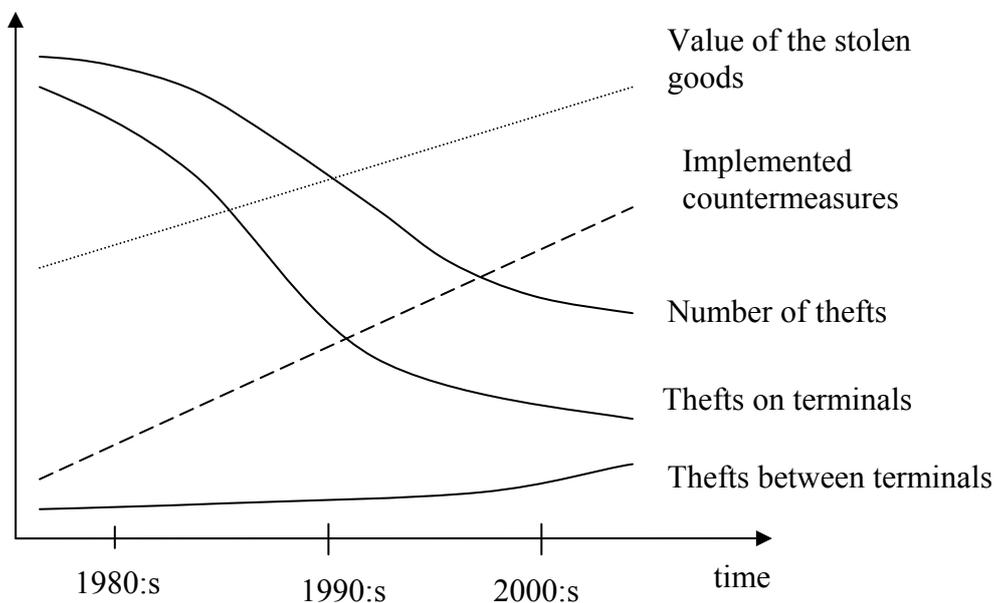


Figure 4: General trends for cargo theft and logistics security

These trends, based on the interviews, can be generalized in figure 4. All curves shall be seen as a combined model and not as a single absolute representation of that specific development. 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 decline in the number of thefts would be 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.

The same development is also indicated in the ECMT (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% 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% were hi-jacks. The types of 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 thefts of goods during transport is, according to the organisation TAPA EMEA (Technical Asset Protection Association – 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 factor for the problem. Table 1 contains data from TAPA members with regard to reported thefts of goods (Winterburn 2005). The crime displacement theory within the transport network is obvious.

	2001	2002	2003	2004
Terminal	36%	29%	22%	17%
Parking	1%	0%	6%	14%
Hi-jacks	8%	11%	13%	13%
Lost during transit	20%	21%	14%	13%
Stolen truck	4%	4%	11%	12%
Jump up	23%	24%	23%	12%
Failed theft attempt	0%	0%	1%	7%
Fraud	2%	1%	5%	6%
Airport	1%	3%	1%	3%
Secure parking	5%	6%	4%	2%
Illegal	0%	0%	0%	0.3%
Total	118	234	334	344

Table 1: Modes of theft per year (Winterburn 2005)

An integrated approach to increase the security in the transport networks

In the transport network there are numerous different stakeholders and they all want to reduce their fraction of the cargo theft problem. One practical way to do this is to ensure that one's own security is better than one's neighbours (referring both to place and product category). The goal is to become less attractive as a target for the perpetrators (Dingle 2005). This practical way to adapt oneself to the need for security within the transport network only contributes to move the problem of cargo theft around, according to the crime displacement theory.

The lack of an integrated approach to security in the transport network became obvious for the business itself in the beginning of the 1990s. One response is the Technology Asset Protection Association (TAPA). It is an association of security professionals working with the transport of high-value products. The reason behind the founding was to increase the protection from theft incidents before the problem became too large. TAPA has developed a certification procedure to help companies improve their security. The certificate is called Freight Security Standards (FSR) and addresses security issues mainly in terminals it has three different levels, A to C where A is the highest. The certification is in Europe performed by an independent auditor. To address the problems that occur outside the terminals TAPA has developed an additional programme called Trucking Security Requirements (TSR). This is a compliance program and is carried out by a self-assessment. In the context of this paper TAPA is an organization which tries to reduce the vulnerability of the transport network by eliminating soft spots and weak links on the mission to reduce theft opportunistic in the supply chain.

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. This disturbance can have two different effects on the flow, namely stoppage or drainage, and it is the stolen volume, related to the total volume, that determines which one of the two effects a cargo theft will bring to the 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 that the perpetrator will seek 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. The six displacements are the result of a change in the total theft situation, especially after a change for the purpose of preventing crime, which generally is implemented to reduce theft in a special part of the transport network. The result is a direct correlation between preventive countermeasures, the potential perpetrator's reactions and the need for an integrated system approach in order to obtain an absolute reduction of cargo theft incidents. The theory of crime displacement in the transport network explains why the absolute reduction is hard to

achieve if an integrated systems approach is not used to secure the effectiveness of countermeasures for the whole supply chain.

References

- Barr, R. and Pease, K. (1990), "Crime placement, displacement and deflection". In Tonry, M and Morris, N (eds.), *Crime and justice*, Vol. 12. Chicago: University of Chicago press.
- Barth, Steve and White (1998), "Spy vs spy". *World trade*, November 1998.
- Bodman, P. and Maultby, C. (1997), "Crime, punishment and deterrence in Australia". *International journal of social economics*. Vol 24. pp 884-901,
- Chapman, P. and Christopher, M. and Juttner, U. and Peck, H. (2002), "Identifying and Managing Supply Chain Vulnerability". *Logistics & transport focus*, Vol.4, No. 4, pp. 59-64.
- Christopher, M. (1998), *Logistics and supply chain management*. Prentice Hall London.
- Christopher, M. and Lee, H. (2004), "Mitigating supply chain risk through improved confidence". *International journal of physical distribution and logistics management*, Vol. 34 No. 5, pp. 388-96.
- Christopher, M. and Peck H. (2004), "Building the resilient supply chain". *International journal of logistics management*, Vol. 15 No. 2, pp. 1-13.
- Clarke, R. V. and Cornish, D. (1985), "Modelling offenders decisions: A framework for policy and research". In Tonry, M and Morris, N (eds.), *Crime and justice*, Vol. 4. Chicago: University of Chicago press.
- Clarke, R. V. (1992), *Situational crime prevention: Successful case studies*. Harrow and Heston, New York.
- Clarke, R. V. (1995), "Situational crime prevention". In Tonry, M and D.P. Farrington (eds), *Building a safer society: strategic approaches to crime prevention*. Chicago: University of Chicago press.
- Clarke, R. V. and Homel, R. (1997), "A revised classification of situational crime prevention techniques". In Lab S. P. (ed.) *Crime prevention at a crossroads*. Andersson Publishing Co Cincinnati US.
- Cohen, L. E. and Felson, M. (1979), "Social change and crime rate trends: A routine activity approach". *American sociological Review*, Vol. 44, pp. 588-608.
- Crawford, A. (1998), "Crime prevention and community safety: Politics, policies and practice". Longman London.

- Dingle, J. (2005), "Displacement theory". *Cargo security international* Vol. 3 No. 5.
- EC - Consultation paper (2003), "Freight Transport Security", European Commission, Brussels.
- ECMT (2002), "Crime in road freight transport". OECD Publication Service, Paris.
- European conference of ministers of transport council of ministers (2001), "Theft of goods and goods vehicles". CEMT/CM(2001)19, Lisbon.
- Felson, M. and R.V. Clarke. (1998), "Opportunity makes the thief: Practical Theory for crime prevention". Home office police and reducing crime unit: London.
- Finch, P. (2004), "Supply chain risk management". *Supply chain management: an international journal*. Vol. 9, No. 2, pp. 183-196.
- Giunipero, L. and Eltantawy, R. (2004), "Securing the upstream supply chain: a risk management approach". *International journal of physical distribution & logistics management*, Vol. 34, No. 9, pp. 698-713.
- Hesseling, R. (1994), "Displacement: A review of the empirical literature". In *Crime Prevention Studies* Vol 3, ed. R. Clarke, 197-230. Monsey, NY: Criminal Justice Press.
- Juttner, U. (2005), "Supply chain risk management: Understanding the business requirements from a practitioner perspective". *The international journal of logistics management*, Vol. 16 No. 1, pp. 120 – 141.
- Lab S. P. (2000), "Crime prevention: Approaches, practices and evaluations". fourth edition. Andersson Publishing Co Cincinnati US.
- Lambert, D. and Stock, J. (1993), "Strategic logistics management". Richard D Irwin Inc, US.
- Lumsden, K. and Dallari, F. and Ruggeri, R. (1999), "Improving the efficiency of the Hub and Spoke system for the SKF European distribution network". *International journal of physical distribution & logistics management* Vol. 29 No. 1, pp. 50-64.
- Mangan, J. and Lalwani, C. and Gardner, B. (2004), "Combining quantitative and qualitative methodologies in logistics research". *International journal of physical distribution & logistics management* Vol. 34 No. 7, pp. 565-578.
- Mason-Jones, R. and Towill, D.R. (1998), "Shrinking the supply chain uncertainty circle". *The Institute of operations management control magazine*, Vol. 24 No. 7, pp. 17-23.
- Mayhew, C. (2001), "The detection and prevention of cargo theft". Australia institute of criminology, Canberra.

- Mishler, E. (1986), "Research Interviewing". First Harvard Press, Boston.
- Nowotny H. and Scott, P. and Gibbons, M. (2002), "Re-Thinking Science". Blackwell Publishers Ltd, UK.
- Popper, K. (1959), "The logic of scientific discovery". Routledge London.
- Repetto, T. A. (1974), "Residential crime". Cambridge, MA: Ballinger.
- Repetto T. A. (1976), "Crime prevention and the displacement phenomenon". *Crime and delinquency* 22: 166-177.
- Sheffi, Y. (2001), "Supply chain management under the threat of international terrorism". *International journal of logistics management*, Vol. 12, No. 2, pp. 1-11.
- Stefansson, G. (2004), "Collaborative Logistics Management". Chalmers Gothenburg.
- Stock, J. R. (1997), "Applying theories from other disciplines to logistics". *International journal of physical distribution & logistics management*, Vol. 27, No. 9, pp. 515-539.
- Svensson, G. (2002), "A conceptual framework of vulnerability in firms' inbound and outbound logistics flows", *International journal of physical distribution & logistics management*, Vol. 32, No. 2, pp. 110-34.
- TAPA, Technology Assets Protection Association,
<http://www.tapaemea.com/engl/index.html>
- Tyska, L.A. and Fennelly, L.J. (1983), *Controlling cargo theft*. Woburn: Butterworth Publishers, Boston.
- Zsidisin, G. and Panelli, A. and Upton, R. (2000), "Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study". *Supply chain management: an international journal*, Vol. 5, No. 4, pp. 187-198.
- Wang, J. and Roush, M. (2000), "What every engineer should know about risk engineering and management". Marcel Dekker inc. New York.
- Winterburn, R. (2005), "A review of 2004 freight crime using TAPA EMEA IIS data". *A presentation in Brussels – February*.

Paper B

Differences in Black and White Logistics System Design

Daniel Ekwall

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

Abstract

Purpose – The purpose of this paper is to analyse the similarities and differences in the design of logistics systems with respect of the legality of the transported goods. This means that the legality of the goods is a vital factor when it comes to take the goods from point-of-origin to the customer. By means of a systems analysis approach based on cases and supply chain theory, this paper discusses the elements that constitute the respective logistics systems design due to legality.

Design/methodology/approach – The method of this paper is inductive. This means that from the description of a black logistics system this paper demonstrates similarities and differences with regards to applicable valid logistics theories. The inductive process will generate a hypothesis. The hypothesis is then compared to the system or context from which it evolved, by means of five case studies.

Findings – The two systems, legal and illegal, are not always separated and may in some circumstances be concordant with each other, where the black logistics system will act as a parasite. Information is the key to unlock the cross-over activities between the legal and the illegal logistics systems, but if the information is used wrong or insufficiently black logistics players only adjust and continue their illegal business as usually.

Research limitations/implications – The information about the black logistics is all from official reports and interviews with security personnel or personnel with similar assignments. This means that the black logistics description is based on secondary data instead of the preferred primary data.

Practical implications – The inducement of anti-terrorism programme like the Container Security Initiative will also have a big impact on the flow of illegal products.

Originality/value – This paper is a step to illuminate the difference's between logistics theories and the reality with regards to the legality on the goods itself.

Keywords: Logistics, Transport system, Transport network configuration, Cargo crime, Logistics system design

Paper type: Research paper

Background

The foundation in all trade is the ability to move or transport the product from the source to the customer and still make a profit. The foundation in all businesses can be described as the two fundamental major tasks, to find or create demand and to supply it. The supply side can further be described as the question of how to produce or how to acquire parts of or the complete product. 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 to acquire goods to meet the customer's demand. This means that the logistics setup or supply chain design differs according to the legality of the trade as well as to the normal economical factors like cost and revenue. Figure 1 illustrates the produce/acquire dilemma from a legal point of view.

Acquire	Purchase of wholesales goods	Theft of wanted products
Produce	Manufacture	Manufacture of counterfeited products / non-intellectual rights
	Legal	Illegal

Figure 1: Matrix of production/acquisition vs. legality of the business

If a company decides to produce or acquire can be seen as a risk assessment strategy based on a cost-benefit analysis. It is normally agreed that a larger business risk will require a larger expected profit. The business risk is commonly stated, the likelihood for an adverse event combined with the economical impact from the event. The risk profile of a certain business is reflected in the minimum margin of profit that is required for someone to realize the transaction. Regardless of which side of the law in a produce/acquire situation a business is, the practical realization of the business needs logistics activities. The design of these activities varies with the legality of the trade.

Research question and method

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. This means that the legality of the goods is a vital factor when it comes to taking the goods from point-of-origin to the customer. Does illegal logistics have the same problem as legal logistics and, if not, is the difference limited to the risk for detection by legal authorities? Will this mean that the illegal

logistics system must be more flexible and adaptable to the market demands than the legal logistics system is? The method of this paper is inductive. This means that from the description of a black logistics system this paper shows similarities and differences with regard to applicable valid logistics theories. The inductive process will generate a hypothesis about black and white logistics systems. The hypothesis is then compared to the system or context from which it evolved (Popper 1959) by means of five case studies. This paper uses triangulation methods to increase the credibility of the results (Ellram 1996). Credibility is substantiated by using a mixture of quantitative and qualitative methods as well as several independent statistics sources, so called methodology triangulation (Mangan 2004).

This paper takes a top-down perspective on the difference between legal and illegal logistics activities. Logistics is seen as more than the sum of all activities. It is seen as a whole system with parts or functions that interact with each other in ways that make them more than just the sum of them all. The most important in a system is 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 demarcation that will contribute to the supply chain design. This means that all the models that are used in this paper are from logistics or supply chain management. The purpose of this paper is twofold, first to categorize what differs between logistics with regard to how risky (in legal terms) the transport is and to create a model that explain how black and white logistics systems interact with each other. This is done by analysing different kinds of illegal logistics activities to find out how and why they differ, both from each other and from the legal logistics system. One great advantage of using the system perspective to analyse this field is that it provides full understanding of the interacting problems that easily appear in complex systems. The majority of all complex systems indicate a large amount of redundancy and by using this redundancy it is possible to simplify the system and thereby both get understanding and the ability to control them (Waidringer 2001).

Data sources and their reliability

The information about the black logistics is all from official reports and interviews with security personnel or personnel with similar assignments. This means that the black logistics description is based on secondary data instead of the preferred primary data. Primary data in this field is very hard to get. The secondary data that is used is collected by trustworthy institutes like FBI, DEA, Europol and the European Commission. In some cases the report is from a trade association, principally regarding counterfeited products. The interviews are made with the purpose of getting examples of black logistics that uses a white logistics flow. The problem here is that the only examples that are mentioned are those that have been discovered and not those that escapade attention. This leads to that in real life black logistics is better than this research states, because most of the used examples are failures, in one way or another.

The black market and its logistics

The black market is 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). In the black market there are several different commonly known 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 buyer of these illegal products is everywhere (Johns 2003).

This market can in many cases be called the gray market due to the fact that the customers do not know if the product is legal or illegal. Bucklin (1993) defines it as follows, "Gray market goods are genuinely branded merchandise distinguished only by their sale through channels unauthorized by the trademark owner." The gray market is the main target for counterfeited product and that market has become global during recent years (Myers 1999). Everything that has been produced can be produced again, by someone else. In terms of contraband it means simply that everything can be a counterfeited product (IACC 2005). In order to bring the counterfeited products from the production site to the end user they are compelled to cross several national boundaries (in general) and ignore intellectual property legislation. The counterfeiting business evolves constantly within current trends and technology (Eca).

The logistics activities involved in cargo crimes are growing in importance, just as the ability to change production type to reduce the risk for detection. The major players in cargo crimes try to produce a diverse range of objects to avoid suspicion from both customers and authorities. A counterfeited product is no longer possible to spot by sight only (IACC 2005). The fake products are nowadays so good that it is often necessary to perform a chemical analysis of the product before knowing if it is a fake or not (EC b). The supply to different black markets can come from cargo crime, smuggling, and 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).

The illegal drug traffic into the US goes mainly from South America. The smugglers use land, sea and air routes to get past the US authorities. The drug cocaine enters the US primarily from Mexico estimated 65% of all cocaine in the US comes this way, but the most recent trend is to transport through the Caribbean; Puerto Rico, the Dominican Republic, and Haiti. This is due to the lack of law enforcement in these locations. The whole distribution of cocaine is controlled by Colombia based organized crime but in recent years it has started to cooperate with Mexican criminals in order to streamline the logistics and to share the risks. The Colombians have organized their operations in a business-like manner, creating cells for special purposes like warehousing or transport. The Colombians have started to cooperate with different groups of organized crime even in Europe, foremost with the Russian mafia, for the supply of cocaine to the EU area (DEA webpage).

The gray market involves the diversion of goods from legitimate supply chains (Huang et al, 2003). In a logistics perspective, black logistics works in the same way as white logistics. 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 illegal production units are placed where the risk for detection is low, combined with the normal white business problem of where to produce its products, considering different types of costs and quality aspects. The black logistics uses the trade routes and port activities in the same way as legal logistics does. Among the receiver countries Europe and the US are favourites, just as Africa is the favourite for transit activities for the black market players. Confiscated products that have not been produced in Africa, like jewellery and CDs shows this, because the African market does not have the ability, in general, to buy that type of products. Countries in Central and South

America act like magnets for counterfeited products. Purchases of counterfeited goods in order to launder money occur there in larger numbers than anywhere else in the world (EC b). Large stocks of illegitimate products are easily shipped from parts of South America to Central America there they are big consumers of that type of products. 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 markets 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).

The Black logistics uses the flow of containers to transport commercial counterfeited products all over the world. The criminals try to delude the customs' watchfulness by "breaking" their way through from the area of production to the area of supply, avoiding direct paths that are well known to the authorities. This tactic is called "breaking bulk" and attempts to conceal the origin of the shipment by having it pass through several other areas (even free trade zones in large ports) and thereby focusing the customs' attention on the latest source origin. With this tactic counterfeited goods produced in Asia are transported by boat to a country known for not making any counterfeit products. There they reload the goods and continue to the market country by plane or other means of transport (EC b). The illegal products make their way back to the white side normally thought flea markets, pawnshops, jewellers, websites or second-hand stores, all depending on who is the seller (Johns 2003).

Similarity between black and white supply chains

The scope for logistics is all activities from sourcing to sales with the aim to supply the customer in a specific marketplace with the right product at the right time (Christopher 1998). The chain of operations, information, companies and payment that is needed to successfully fulfil the scope of logistics is called supply chain management. In figure 1 this is explained in a simplified way, from a company perspective and with only one supplier and one customer.

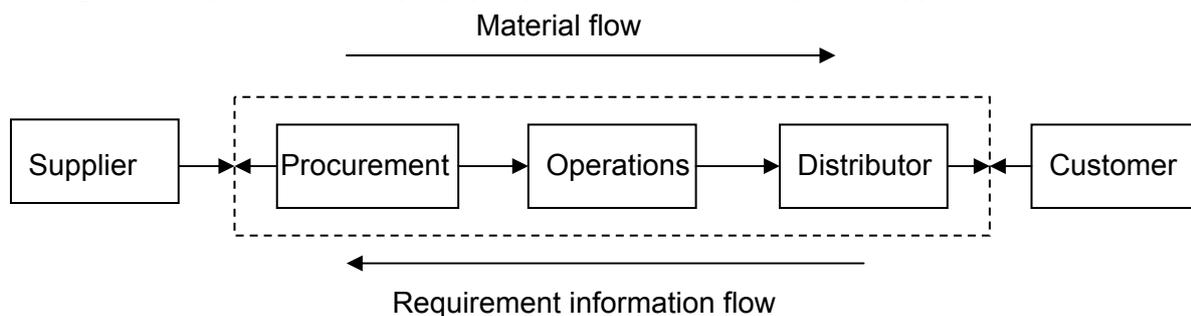


Figure 1: The total logistics system concept (Christopher 1998)

The reality is far more complex. It is useful to talk about supply networks instead of chains, but every link in the network is like a chain so therefore the term supply chain is used. Regarding black and white logistics in a supply chain context they are both similar and different from each other. At an abstract level it must be able to describe both black and white supply chains in the same way and with the same elements. But at a concrete level they differ in the characteristics and design, which depends on the different surroundings where they act. In figure 1 five boxes are used in four of which there are different activities which lead to a successful delivery of a product to a customer. Let us take a closer look on these four activities with regard to how they may differ between black and white logistics systems.

<i>Activities</i>	<i>Logistics system concept</i>	
	<i>White</i>	<i>Black</i>
Supplier	Is chosen on criteria as cost, quality, reliability etc.	Can be same as white but it depends on the logistics wanted goods
Procurement	The procurement process in a white company is considered a key function.	Works in the same way as in white business with questions like price, quality, and supplier performance but also with a detection parameter.
Operations	Can be lean, agile, traditional or according to any production theory.	Same as in white logistics, but with a detection parameter.
Distribution	Is chosen on criteria as cost, quality, reliability, speed etc.	Is chosen to get the lowest possible risk for detection in combination with the white logistics factors. The detection risk factor is decisive for the transport setup.
Customer		The “same” as in white logistics

Table 1: Black and white logistics system concept comparison

The big difference between black and white supply chains is in the distribution element of the supply chain. The distribution is achieved with a transport system. If the big difference between black and white logistics systems is found here, what is the cause of that difference?

Transport system in general

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. This is the cause or the reason for the existence of the whole system, the aim of which normally is to move material from one place to another. 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.

If black and white logistics work in the same way this means that they both can be describe in terms of the four flows and the three levels of logistics. Black and white logistics can use the same resources at the same time but black logistics can also create its own infrastructure. The method that is used depends on the overall risk with the transport. Higher risk leads to the creation of new infrastructure or innovative use of resources.

The complexity in logistics can be explained by displaying the four different flows that are always involved in logistics activities. The flows of material and resources are already 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 1998). The four flows of logistics between consignor and consignee are shown in figure 2. These four flows can all be used to illustrate the difference between black and white logistics because all flows must be involved in the logistics activities. This

implies that they can all be used to separate black flows from white flows and therefore also to detect illegality in the logistics business.

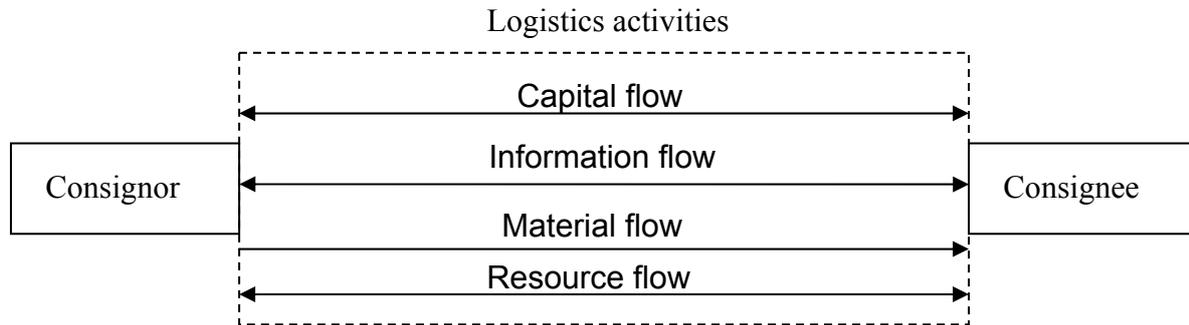


Figure 2: The four flows of logistics (Lumsden 1998)

Transport system configuration depends on risk assessment

The risk for detection is directly linked to the type of goods that are being transported and the geographical area where the transport takes place. This is one basic theory that can be drawn themselves from the data on the black market and its use of black logistics. The goods indicate that if it is easy to detect if the product is illegal, it must be concealed very carefully or ship another way. A good counterfeited product that is very hard to distinguish from an original one, gives the possibility to send it as a legal product in the legal logistics system. In the shipments of the modern world is it unlikely that a single transporting unit carries only contraband products (Naylor 2004). If we then look at the margin of profit combined with the weight and volume of the product, this difference becomes more obvious. Products with a high margin of profit and small weight/volume that is without doubt illegal are more likely to use a separate logistics infrastructure. The use of a smugglers harbour is generally more common in drugs than among trade with counterfeited products. This depends on the detection risk connected to each goods type. The authorities first look for the products but also for the resources that carries them. If they can find them they prevent the transport but it is virtually impossible to check all transport in the world, so they need a smart method to figure out where to look. The second way to find illicit transport is by checking information and to follow the monetary trace. The undercover work and informer activities that police and customs work with are a way to get information about the transport so that they can inspect the right ones. If we look closer at the different types of goods in view of the four flows and the three levels in logistics, we can get a better understanding of how they differ. This is presented in table 2.

<i>Flow or level in logistics</i>	<i>Type of goods</i>		
	<i>Original</i>	<i>Counterfeited</i>	<i>Undisputedly illegal</i>
Material	Uses the White logistics system	High quality products of this type is nowadays extremely difficult to separate from originals	This type of goods is normally easy to recognize, especially for professionals. There is the risk detection factor high.
Resource	Uses the White logistics system	Uses the White logistics system, often a full truck	Uses sometimes the white system but is often

		load or container with this type of product	shipped with special vehicles or in special prepared containers
Infrastructure	Uses the White logistics system	Uses the White logistics system	Often in the same infrastructure but other routes or shipping methods (bulk breaking) than white logistics normally use
Information	Correct	False but as little as possible	None or false (completely)
Money	Legal transactions	As legal as possible, can be disguise in real legal transactions	Uses cash as secret as possible. To trace the money is a good way to find the goods

Table 2: Transport system configuration depending on product type

Cases of black logistics concealed in white logistics

To fully understand the innovative use of white logistics by the black logistics players; it is useful take a closer look at some cases of black logistics. Five different cases of black logistics are presented. Three of them represent a description of a single event and the other two are summarized descriptions of a specific market or the customs view on black logistics.

Case 1: In a major terminal in Sweden there was a break-in and theft of 42 high-pressure wash appliances. During the break-in the thieves checked other containers and trailer, altogether nine load units were checked. Seven of them were untouched, in one container with wine was missing one box and finally the 42 high-pressure wash appliance were missing. The terminal was guarded by fences, a surveillance camera and security personnel. The surveillance camera was put out of business by a professional, the four right cables of the right camera were cut off in a professional way. The theft was done by professionals (the report states that they were at least three perpetrators) but the black market value of the 42 high-pressure wash appliances is not higher than 4000 Euro. The whole set-up indicates that the boxes with high-pressure wash appliances contained something more than just high-pressure wash appliances (Inbrottsutredning 2003). The real target for the thieves probably was some kind of drugs. This method provides the thieves with the advantage that the police had to prove that they knew there was something else inside the high-pressure wash appliances.

Case 2: A major logistics company in Sweden discovered a few years ago that a shipment sent from Portugal to Sweden did not have a correct receiver address. The sender could not be located. After trying to deliver the box a few times they opened it to get more clues about who should have it. The shipment contained drugs. The logistics company called the customs and the police in order to investigate the shipment. The consignment note stated that the box contained machine parts (Interview Lundkvist 2005). This type of problem is easy to prevent because a simple check of sender and receiver will quickly tell if both of them exist and have made any earlier shipments.

Case 3: The same logistics company (as in case 2) in Sweden provides third-party logistics. A liquor shipment arrived from continental Europe to Stockholm with one of their well known

customers as addressee. When the truck came to the delivery address which was the customers headquarter instead of his warehouse. The customer did not know about the shipment but redirected the truck to the logistics provider warehouse. When the truck arrived they discovered that all the papers round the shipment were fakes and that the goods were not a liquor brand that they represent at all. The criminals smuggling the alcohol were presumably planning on changing the delivery address while the goods were on their way (Interview Lundkvist 2005).

Case 4: The trade with objects 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, a very unwilling supplier. China has hard 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 paper work of artefacts origin) and shipped to the buyers market in Europe and the US. The big problem with this type of black logistics is that it is very hard, almost impossible; to prove that the artefacts are stolen, because the only real proof that exist is the hole in the ground from which it was dug up. In an international logistics view the actors want to mix legal (correct paper work) and doubtful objects together in the same shipment to make it even harder to prove illegal activities (Interview Lundén 2004).

Case 5: The Swedish custom categorizes the smugglers (actors who bring illegal products into or out of Sweden) in 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 break a law (in cases of counterfeited products, not drugs). The large scale smuggling has good knowledge about both logistics and customs routines. They try to be anonymous in the eyes of the law or use goxies and front companies as importers. If it is about counterfeited products, the pure quality of the counterfeited products is much better then the one that small scale operates with. Large scale smuggling uses Sweden on a regular basis as a transit country for the goods. When the goods are drugs it happens that 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 (Interview Helsing 2005).

Categorization of the five cases

All five cases state that the use of false information (to some extent) is very useful. In the first case the black logistics use the “Cuckoo in the nest” method, which means that someone places goods inside another shipment that no one else knows about. The logistics company never knew that the load contain more and illegal goods. The big question in that case is how and where the illegal goods came in the load with high-pressure wash appliances in the first place. Many of these problems would be avoided if the container hade tamper-proof seals to prevent that the planting of the illegal goods or theft of the legal goods can occur. This still leaves the possibility of fiddling with the goods or container in the terminals, but there is it easier to watch over both goods and personnel, than during transport. This case is a good example of how innovatively black logistics can use a legal shipment. Case 2 shows that if only the most basic information check was done, some problems with black logistics were easily avoided. The third case indicates that the black logistics service intermediary fakes the receiver in order to make the logistics service provider perform the actual transport and meanwhile use the service/possibility to change place for the delivery.

The cases 4 and 5 both show the complexity and the difficulty to prohibit black logistics from using the legal logistics system. The fourth case proves two things vital for black logistics, flow pollution and the importance of being able to track the goods from its source. If the authorities can not prove that the product is illegal, it is considered legal. This is what both flow pollution and non-existing (documented) origin are all about. The last case shows a big difference between professionals and amateurs regarding black logistics activities. The professional acts as the unseen link in the shipment. He pulls the strings and stays out of sight from the authorities. He also uses the method of bulk-breaking to disguise the origin and thereby deluding the customs of the source (country) of the shipment. The problem with counterfeited or faked archaeological artefacts is the lack of originals to compare the fake with. This problem makes it even harder to distinguish fakes from authentic artefacts. The customs can not have the expertise needed to spot these fakes in every customs station, but in the case of counterfeited industrial products they have more of this knowledge, both which brands and also which products that are more likely to be counterfeited.

Triad logistics setup in terms of black and white

When shipping the illegal product to the customers, to avoid discovery the black logistics service provider will normally use a regular flow and a legal logistics company. The forwarder may not be aware that the products are illegal (cases 1-3). The choice of illegal logistics service provider is basically made in the same way as the legal business stakeholders do, considering price, time and reliability plus the possibility for the shipment to reach the market undetected. For counterfeited products or other types of goods where it is difficult to see whether they are legal or not, black logistics tries to use the white logistics system for its transport needs because it is cheaper than to create and manage a separate system. Neither the sender nor the receiver wants the logistics company to know the real truth about the cargo. In terms of logistics theory, how does black logistics solve this problem?

If the four flows of logistics are presented in a supply chain context, we can look at one link between two companies, places or organizations and add the logistics service provider (LSP). We get the logistics triad setup. This model focuses on the relationship between shipper, buyer and logistics companies. The foundation of the logistics triad is a cooperative, three-way relationship with the movement of goods as the core (Stefansson 2004).

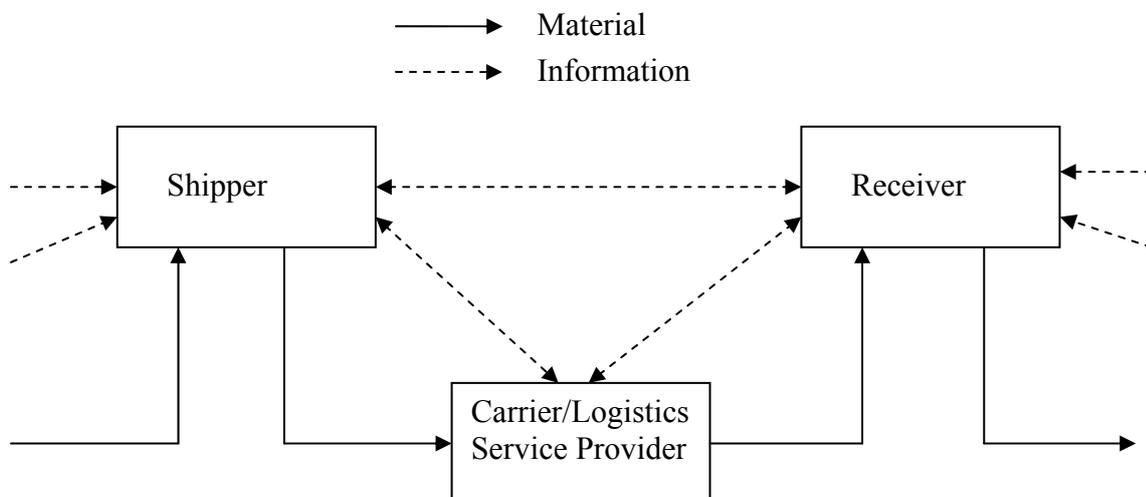


Figure 4: The logistics triad (Stefansson 2004)

In black logistics the white LSP can be unaware of the role it plays in the black logistics triad. This means that the shipper or receiver does not provide the LSP with correct information or not at all (cuckoo in the nest). But in case the role of LSP is played by organized crime as the black LSP (BLSP), black logistics works with the same logistics triad setup as the white logistics does. If the goods are illegal in one way or another (type, volume etc in one or more territories that the shipment passes) the method of smuggling is commonly used. Smuggling means that the BLSP tries to control the shipment in a way that reduces the risk for detection to the lowest possible. This can mean that it uses a white LSP and conceals or hides the goods inside other goods or gives it false information regarding goods type, volume, consignor, consignee etc. in order to get the goods to their receiver. To understand the relationship between a LSP and a BLSP it is useful to compare the BLSP with a logistics service intermediary LSI.

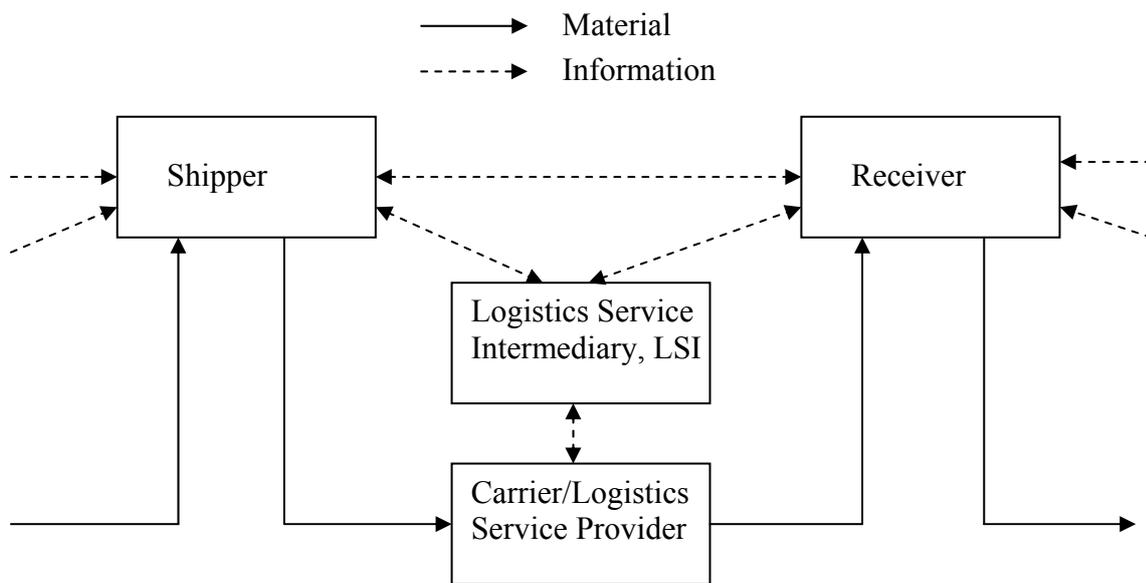


Figure 5: Logistics setup with a Logistics Service Intermediary (Stefansson 2004)

To understand this component it is useful to know that the white LSP does not know that it is being used for illegal shipments. To create this illusion the black LSP uses false documentation and/or hides the real goods inside goods with a disguising purpose. Again the key issue is information.

White business action to separate black from white logistics

The white business companies are naturally not pleased with the situation of competition from black companies. They may not be pleased with legal competition either but that is another question. The strive for better business deals and the general globalization trend, that started centuries ago, have lead to a embedment of illegal actions within legal markets (Naylor 2004). This implies that the old time black markets have been integrated with legal transactions and the markets today can be describe as containing every shade of gray, when referring to the legality of the markets as a whole (Naylor 2004). The white businesses are especially concerned with the problems of counterfeited branded products and theft of their own products. To increase the efficiency in detecting counterfeited products the white businesses use cutting-edge technologies and security actions. Technologies tested are organic DNA, retinal scans, holographic labels and RFID tags (Monks 2004). Technologies used for securing the true identity of the product need to be tamper-proof, The RFID technology is not secure, but organic DNA have this 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 need to be consequent, the harder it is to get away with the usage of false data. It has also been suggested that customers should be educated to easier distinguish a fake from an original. To do this the customers need evidence (serial numbering systems etc.) or very good knowledge about the product. To make it harder to counterfeit products it can be successful to use valuable materials instead of cheaper ones (Hilton 2000).

The Container Security Initiative (CSI) was proposed in early 2002 by the U.S. Customs, now U.S. Customs and Border Protection, as a reaction to the terrorist attacks of September 11. The primary purpose of CSI was to protect the global trading system, mainly the trade lines between CSI ports and the U.S. There are currently 50 CSI approved ports (September 2006). The CSI has four core elements:

1. Using information to identify containers that pose a risk for terrorism
2. Pre-screening those containers that pose a risk at the port of departure
3. Using detection technology to quickly pre-screen containers that pose a risk
4. Using smarter, tamper-evident containers

The objective of the CSI is to make the logistics flows of sea containers more secure. Most of all the CSI operatives are looking for potential terrorist weapons, including weapons of mass destruction. But the CSI can, if used right, be a large asset in fighting smuggling of illegal goods across the world (CBP website).

The problem with cargo crimes is complex and depending on which type of cargo crime that needs to be prevented, different methods have different impact on the problem. When it comes to CSI it has a great potential, if used right, to limit the free movement of counterfeited goods and to prevent theft from containers. But the main reason behind CSI is the opportunity to detect terrorists using the container flow for terror purposes. The positive consequence of the “war against terrorism” is that old fashion cargo crimes have become harder and riskier to accomplish (Littman, 2003). For the white business the CSI can be seen as both a global supply chain headache and a business opportunity, all depending 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 black logistics inside white logistics and to find flows of purely black goods.

The Black and White Logistics model

The logistics activities use the same infrastructure, regardless if the goods can be categorized as legal or illegal. 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 faster to conceal illegal goods in legal shipments, even if the use of special black logistics trade routes still exists in rare cases. Even in black logistics, the need for speed and low cost control sets the general trend in the way of doing business with highest possible profit. Regarding black logistics resources to carry out the actual transport, there still exist trucks with only illegal goods in the shipment, while large types of cargo carriers (ocean going ships) are not likely to use illegal infrastructure but is more likely than a truck to contain some kind of illegal goods. The highest level of logistics, the flow of material, and the difference between black and white logistics is most evident. This is due to the fact that here it is easiest to distinguish legal goods from illegal ones. This possibility varies with the type of product,

the documentation and the means of identification to establish the owner of the product. Therefore black 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 6 marks the vague borderline of where the logistics activities are neither black nor white, but gray. It depends on the difficulty to establish whether the goods are black or white. The box for the LSP (in figure 6) contains all types of activities that a LSP performs.

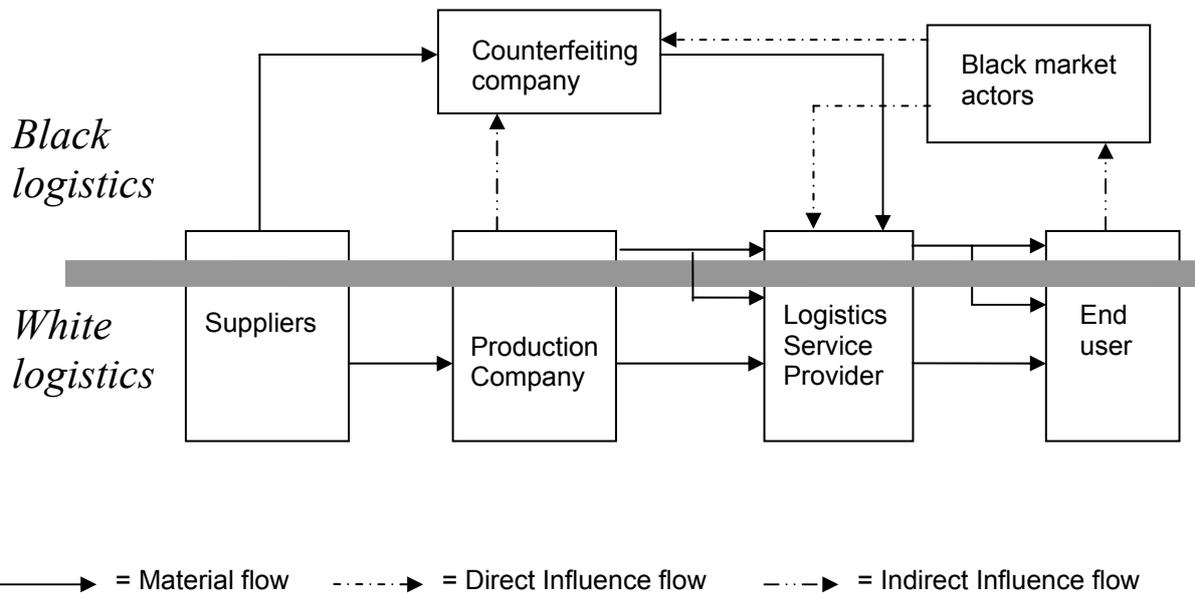


Figure 6: The black and white logistics systems (Author)

To use the potential in the white logistics system for illegal activities it is necessary to have good knowledge about logistics and also to be creative to find new ways to conceal the delivery of goods to the right buyer. The role of Logistics Service Intermediary, who can use the legal Logistics Service Provider for criminal purpose, is taken by organized crime.

Conclusions

All transport or logistics activities in the world can be divided into legal and illegal ones. These different activities together form systems of black (illegal) and white (legal) logistics. One problem is the gray area between black and white logistics that is constituted of different regulations in different countries and limitations in volume depending of the ownership of the goods. This problem is best illustrated with drugs and medication like growth hormone which is illegal for almost everybody to own and possess except for certain medical purposes. So depending on who is the owner or forwarder, growth hormone can be in either black or white logistics.

This paper shows that the decisive difference between black and white logistics is found in information about the products, transport routes, ownership and different domestic laws. In terms of discovering illegal goods in legal logistics flows the need for correct information can not be overestimated. The pure nature of the illegal goods governs the choice of logistics setup, e.g. using concealed shipments or own system. The more difficult it is to establish whether the product is illegal or not, the more likely it is to be transported in the white logistics system. By providing reliable false information to the white logistics company is it

possible to increase the likelihood for the illegal shipment to reach its consignee. Whenever an illegal product is entering the white logistics system there is a cross-over point between the two systems. To prevent this from happening many different methods are required, but common for all methods is the effective use of information. If not prevented, the black logistics will continue to parasitize on its reluctant host. The general reaction of white business to reduce black logistics activities corresponds well to the four flows of logistics. Exemplified by the use of RFID and other types of unique identification on every single product increases the possibility to track stolen goods and makes it more difficult to produce counterfeit products. This strategy could open for the possibility that customs, police and other authorities easier can find counterfeited products. This requires extended co-operation between different stakeholders. The last type of reaction is the Container Security Initiative, which makes both the resources and the infrastructure more secure, simply by making it riskier to transport stolen or counterfeited goods in containers. The biggest contribution that CSI brings to security is its focus on the flow of information and that the information about the shipment is correct. This problem was elucidative in all five cases. It shows how important it is to have the correct information about a shipment. In other words, information is the key to unlock the cross-over activities between the black and the white logistics systems. If the information is used wrong or insufficiently, however the black logistics players only adjust and continue their illegal business.

References

ACG, Anti Counterfeiting Group, <http://www.a-cg.com> (printed 2005-0817)

Badolato, E. V. (2000), "Smart Moves Against Cargo Theft". *Security Management*, Alexandria USA.

Bolan, C. (2005), "How to Catch a Counterfeiter". *Global Cosmetic Industry*, Vol. 173, No 6, Allured Publishing Corporation.

BRÅ-2002:7 (2002), "Organiserad brottslighet": BRÅ (Swedish)

Bucklin, L.P. (1993), "Modeling the international gray market for public policy decisions". *International Journal of Research in Marketing*, Vol. 10 No. 4, pp. 387-405.

CBP, U.S. Customs and Border Protection, www.cbp.gov (printed 2004-12-14)

Christopher, M. (1998), "Logistics and Supply Chain Management". Prentice Hall London.

DEA, U.S. Drug Enforcement Administration, www.dea.gov/concern/drug_trafficking.html (printed 2005-09-13)

EC (1999), European Commission: Counterfeiting and piracy: Munich hearing endorses need for EU action, http://europa.eu.int/comm/internal_market/en/indprop/piracy/munchen.htm (printed 2005-03-24).

EC (a), European Commission: Counterfeit and piracy, Introduction, http://europa.eu.int/comm/taxation_customs/customs/customs_controls/counterfeit_piracy/index_en.htm (printed 2005-03-24).

EC (b), European Commission: Combating counterfeit & piracy, The economic consequences, http://europa.eu.int/comm/taxation_customs/customs/customs_controls/counterfeit_piracy/combating/index_en.htm (printed 2005-03-24).

Ekwall, D. (2005), "Characteristics of cargo theft changes due to transfer effects". *ASIS Security Solutions for the Future*, Copenhagen 17-20 April 2005.

Ellram, L. M. (1996), "The use of case study method in logistics research". *Journal of business logistics*, Vol. 17, No. 2, pp. 93-138.

Europol (2004), "2003 European Union organized crime report". Luxembourg.

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

Huang, J-H. and Lee, B. and Ho, S. (2003), "Consumer attitude toward gray market goods". *International Marketing Review*, Vol. 21 No. 6, pp. 598-614.

Holmes, J. (2004), "Coping with U.S. Customs' Container *Security* Initiative". *World Trade*, Vol. 17, No 4, BNP Media.

Hilton B, and Ju Choi, C. and Miller, C. (2000), "Quality, Counterfeits and Strategy in the Fashion Industry". *Security Journal*, Vol 13, No 4, Perpetuity Press.

Hoover, W. and Eloranta, E. and Holmström, J. and Huttunen, K. (2001), "Managing the demand-supply chain". John Wiley & Sons, New York.

IACC (2005), White paper, The negative consequences of international intellectual property theft . Washington.

Johns, T. and Hayes, R. (2003), "Behind the fence: Buying and selling stolen merchandise". *Security Journal* ,Vol 16, No 4, Perpetuity Press.

Kotler, P. and Armstrong, G. and Saunders, J. and Wong, V. (1999), "Principles of Marketing". Second European edition. New Jersey: Prentice Hall,

Littman, J. (2003), "THWARTING the Perfect Crime". *Electronic Business*, Vol. 29, No 4 Reed Business Information.

Lumsden, K. (1998), "Logistikens grunder". Studentlitteratur, Lund (Swedish).

Mangan, J. and Lalwani, C. and Gardner, B. (2004), "Combining quantitative and qualitative methodologies in logistics research". *International journal of physical distribution & logistics management* Vol. 34 No. 7, pp. 565-578.

Monks, B. (2004), "Counterfeiting: A Crime that Affects Us All". IAEI News The magazine, http://www.iaei.org/magazine/04_c/monks.htm.

Myers, M.B. (1999), "Incidents of gray market activity among US exporters: occurrences, characteristics, and consequences". *Journal of International Business Studies*, Vol. 30 No. 1, pp. 105-26.

Naylor, R (2004), *Wages of crime*. Cornell University Press. Ithaca.

Popper, K. (1959), "The logic of scientific discovery". Routledge London.

Sarnecki, J. (2003), "Introduktion till kriminologi". Studentlitteratur, Lund (Swedish).

Stefansson, G. (2004), "Collaborative Logistics Management". Chalmers, Gothenburg.

TAPA, Technology Assets Protection Association, <http://www.tapaonline.org> (printed 2004-12-14)

Waidringer, J. (2001), "Complexity in Transport and Logistics Systems". Chalmers, Gothenburg.

Wilson, B. (1990), "Systems: concepts, methodologies and applications". John Wiley & Sons, New York.

Zimmerman, E. (2004), "How DNA Can PROTECT YOUR BRAND". *FSB: Fortune Small Business*, Vol. 14, No 10.

Inbrottsutredning 2003: Polis anmälan nummer K72882-03 (Swedish)

Interview 2005-05-04: Per Lundkvist

Interview 2004-02-27: Staffan Lundén

Interview 2005-05-20: David Hellsing

Paper C

The role of temporary storage from a supply chain perspective

Daniel Ekwall

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

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 from a supply chain perspective. The primary research question is what purpose or role temporary storage takes and whether the temporary storage concept can contribute to reducing risks and uncertainty in the supply chain.

Design/methodology/approach – The research method is deductive; hence a hypothesis is developed by logical deduction from existing theories. The perspective is a system theoretical approach towards logistics.

Findings - The temporary storage is located between nodes in the transport network. The temporary storage function will act as 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. First, better and exacter scheduling of delivery time. Second, 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 these reductive measures can work together, and as a combined toolbox they can contribute to reducing the risk and uncertainty in the supply chain.

Research limitations/implications – The use of the deductive research method limits the research results to become more of a general guide-line. To realize them needs more research to establish all consequences from implementing the three identified categories of solutions.

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.

Originality/value – This paper illuminates the purpose and the drawbacks of temporary stops in the flow of goods within the transport network. There is 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

When people drive through the country and come close to an industrial area filled with factories, warehouses and terminals they have become used to seeing several trucks in parking lots or at the road-side, waiting for loading and unloading opportunities. A similar view meets everybody who enters a seaport, regarding the volume of containers, trailers and trucks that wait there. The use of these waiting places has increased in recent years.

Research and method question

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 takes and whether the temporary storage concept can contribute to reducing risks and uncertainty in the supply chain. The research method is deductive; hence a hypothesis is developed by logical deduction from existing theories. This helps to substantiate the objectivity of this research (Popper, 1959). The perspective of the research in this paper is from a supply chain and the associated risk. Thus the context of the paper is supply chain management and the scientific field is logistics. The developed deductive hypothesis on temporary storage is then compared with the context of the research.

Supply chains' associations with risks and uncertainty

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 that co-operate to fulfil the scope of logistics is called the supply chain. The reality is however far more complex.

Historically, security and vulnerability within the supply chain were largely neglected until the terrorist attack at the World Trade Centre. The subjects of supply chain 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. 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). Towill (2005) illuminates that all players in a supply chain are exposed to risk from demand uncertainty. 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. The concept of risk combines probability and consequence for a certain event. Juttner (2005) states that risk-taking is generally perceived as an inevitable aspect of supply chain management.

One way to reduce uncertainty in the supply chain and still keep stock holding cost at a decent level is the VMI strategy (vendor-managed inventory). This is achieved by the supplier handling the raw material stock at the customer's facility (Disney et al., 2003). Another useful concept when dealing with a demand lead time that is shorter than the production process is the customer decoupling point. Basically it aims to induce a point or position that decouples

the demand volatility from the production processes (Hoekstra et al., 1992). This means that upstream from the decoupling point the processes are controlled and performed according to forecasting, while downstream they are performed according to customer orders (Wikner et al., 2005). Thereby the supply chain receives higher uncertainty (in forecasting) but reduces the risk of producing or positioning the wrong product. The endeavour to centralize inventory is also affected by sales uncertainty (Zinn et al., 1989). However, the most dangerous source of uncertainty is market volatility. This uncertainty is addressed by marketing activities and agility of the supply chain (Sabath, 1998).

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. 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). 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).

Therefore the demand and supply risk sources address disturbance in physical distribution, through in- and outbound logistics activities. Risk consequences can be either 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 can also 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 disruption effect associated with risk and uncertainty in the supply chain related to global sourcing is demonstrated as longer and more variable lead times, quality variance, shipments in consolidated volumes, large physical distances, cultural differences and low information exchange (Das et al., 1997).

The causes for a risk can be either deliberate or unintentional. Unintentional ones are normally called process failures while the deliberate ones are antagonistic risks to the supply chain. In the manufacturing sector the loss from process failures were 78 percent of total stock loss year 2000, but in the retailer sector has this amount drop till 27 percent (ECR, 2001). This shall be compared with the deliberately caused stock losses of 22 percent in manufacturing and 73 percent in retailing of the total stock loss year 2000. These figures are divided in three categories, namely supplier fraud (0 percent and 12 percent, respectively), internal (11 percent and 24 percent) and external (11 percent and 37 percent) theft (ECR, 2001). These numbers indicate that the closer to the end user the products come in the supply chain, the greater is the risk for deliberately caused stock losses. The first step a company needs to take is to accept that a stock loss can lead to lost sales, thereby affecting the profit (Beck et al., 2003).

Risk management or security methods to reduce disturbance

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 associated with that probability. Attempts to minimize the own business risk have always been a part of doing business. But minimizing the business risk often also leads to minimizing the profit. Risk management comprises different methods that strive to balance risk versus profit and cost. This should be compared with the use of security, which in general terms means that 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. This comes from the fact that 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 address unlimited risk sources to achieve a reduction of the total risk (Manunta, 1999). Most risk management methods are based on statistics (obtained by various methods) and 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 is the traditional risk management approach for reducing disturbances. 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. Therefore traditional risk management can not deal effectively with the dynamics of antagonism, which is the area for security. The causes for antagonism can be described as a spiral of inputs, processes and feedback, which explains the dynamics of antagonism. This dynamics tends to make the analysis, assessment and decision very complex, and the world seems to be anything but deterministic (Manunta, 1999). Manunta here argues that security and traditional risk management are opposite to each other. This is a too limited view. Both approaches aim to reduce causes and consequences of an adverse event. By including ideas and mindsets from security into risk management approaches, they will be able to deal with antagonism. The understanding of the antagonistic dynamics is vital for an analysis of where, when and how the protector shall be present to prevent adverse events from occurring. The security version of risk management needs to address the dynamics of antagonism by understanding the environment or the context of the threat. Therefore contextual risk management approaches address dynamic risk sources, while statistical risk management approaches are more appropriate for static risk sources. Contextual risk management can thus be seen as intelligence (Manunta, 1999).

Most types of disturbances are not caused by deliberate action, like theft and sabotage. If that would be the case, the disturbance-reducing methods used by companies in the business should address criminal behaviour or dynamics of antagonism toward transport in general. This is not the case. Therefore is it likely that the main types of disturbance are unintentional or process failures that occur with different degrees of predictability. This is actually not the case when it comes to demand alteration or demand risk sources. This type of disturbance are 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 they were 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 is the risk management approach for reducing disturbance. 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 occur. Therefore security can be seen as intelligence, instead of equations, which contain probability and effect, as in risk management (Manunta, 1999).

Everything that happens in a system the makes it vary from the ideal status is generating uncertainty throughout the system. In risk management terms can this be described as if the cause and the effect are known then can the proper countermeasure or the right plan of action be used. If there is uncertainty within the system it will delay the starting point for the proper plan of action. Therefore can uncertainty be seen as a delay function 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 of a cargo incident is illustrated in figure 1.

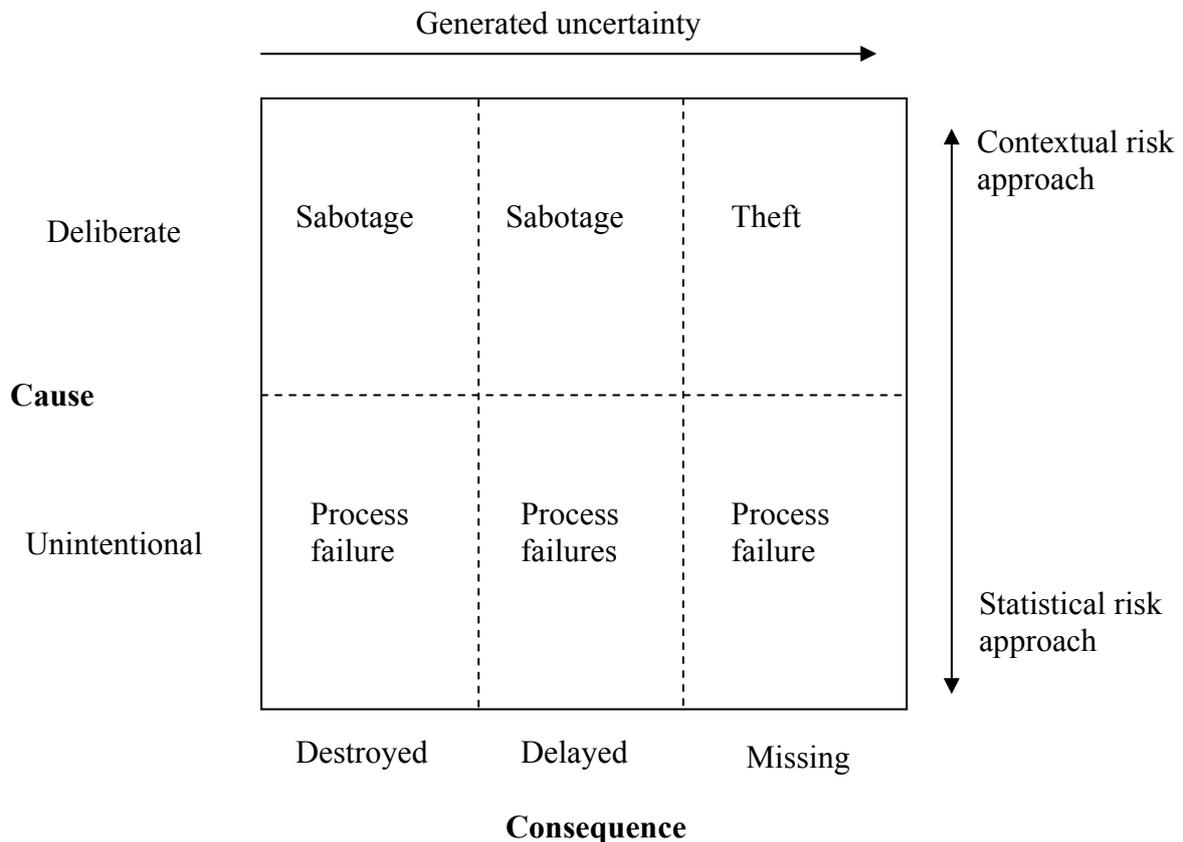


Figure 1: Cause/consequence matrix for cargo incidents

The literature in logistics agrees that uncertainty shall be reduced as far as possible (Nilsson, 2006). The basis of this idea is that there exist an equilibrium and stability in all logistics (Lambert, 1998). In other words, everything can be controlled. But if the risk is caused by deliberate actions then there is no stability. Nilsson (2004) states that with regards to uncertainty and complexity do logistics researchers and practitioners need to “go with the flow” instead of trying to remove all uncertainty. In terms of security and risk management in

supply chain does Nilsson imply that both a statistical (stable) and a contextual (complex) approach are needed in order to reduce the total risk.

This discussion about the difference and similarities between security and risk management or as states above that security is a different risk management approach, namely contextual instead of the commonly statistical one. According to White (1995) can risk analysis be conducted in two ways, either holistic or reductive. The difference between these two ways is illustrated in table 1.

	Holistic approach	Reductive approach
Method	Systemic	Systemic
Issue tackled by	Investigating the problem's environment	Reducing problem into smaller and smaller parts
Approach characterized by	An upward movement	A downward movement
Simplifies by	Taking multiple partial views	Breaking down problem into simplest parts

Table 1: Table of differences between holistic and reductionist approaches (White 1995)

The holistic approach is like the contextual approach, useful when the risk arises from the environment to the problem and a greater understanding of the cause is needed to be able to reduce the total risk. Likewise are the similarities between statistical and reductive approaches useful when the risk cause is repeatable and recurrent predictable. The antagonistic gateway is a risk that arises from both within and the environment of the transport network and is deliberate abused. Therefore is the contextual or holistic approach better to use than the statistical or reductive. In this thesis is this achieved by focusing on both the potential perpetrator and the transport network and this with theory from both criminology and logistics. This also means that this thesis do not try to break down the problem in simplest parts consequently do it aims to take a wide and multi level analysis of the problem with antagonistic gateways in the transport network.

According to Giunipero and Eltantawy (2003), certain risk management acquisition practices can create new risks and problems. Strategies like single sourcing, just-in-time and a reduction of supply base all have the potential to create disturbance throughout the supply chain. Giunipero and Eltantawy (2003) even point out that the trust in e-procurement tools also brings additional risks to the supply chain. All risk and uncertainty, from a supply chain perspective, will be transferred through a transport network. If designed and used wisely the network can reduce risk and uncertainty. The relationship between supply chain and transport network is illustrated in figure 2.

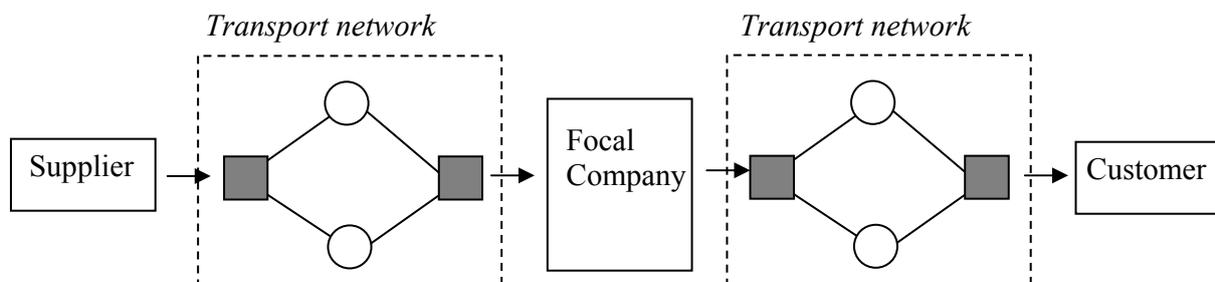


Figure 2: The relationship between supply chain and transport network

Transport network constraints

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). 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). Figure 3 shows a typical transport network with gateways.

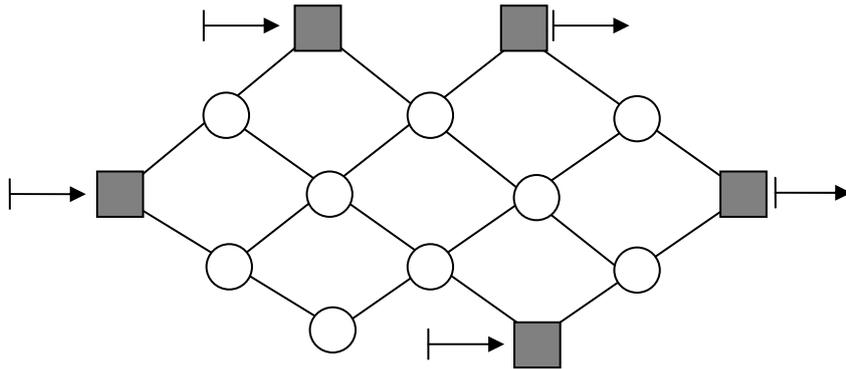


Figure 3: Transport network with gateways

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

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

Geographical concentration of consignors or consignees – A geographical concentration of either consignors or consignees increases the opportunity to co-ordinate pick-up or delivery activities, thereby creating economy of scale in each single 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 that each actor in the supply chain ships or receives each time.

Infrastructure – The network of terminal, harbours, airports, roads and railroads that are used during the transport.

These 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.

Uncertainty and freight transport

The borderline between certainty and uncertainty is much of a greyscale in all business. Certainty in freight transport means that everything goes exactly (literally) according to plan, which never occurs. This means that all uncertainty can not be erased. Uncertainty is simply a key characteristic of any economic activity (von Oetinger, 2004), i.e. uncertainty is always present to some extent in every affair (Sabath, 1998). Too much 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 they are exposed to. Supply chain management is in this context described as uncertainty reduction (Mason-Jones et al., 1998).

According to Prater (2005) the increasing use of information systems, such as ERP, EDI, MRP and DRP, has improved the efficiency for the actors in the supply chain, but at the same their intrinsic uncertainty has also increased. This development depends also on the increasing complexity and competition in today's 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, so 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).

The function of temporary storage

The present trend in leanness and general low inventory levels together 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 done otherwise. Therefore is it vital for every company to find a balance between inventory levels and the risk for disturbance in both in- and outbound logistics (Svensson, 2003). 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 (Das et al., 1997). An increased distance between supplier and buyer also adds uncertainty due to longer lead time and more potential transport disruptions (Giunipero et al., 2003).

According to Giunipero and Eltantawy (2003) most purchasing professionals have, historically, adopted policies and routines to reduce the impact and to prevent future incidents after a certain event already happened. The professionals used multiple supply sources and larger safety stocks. The reason was that risk simulated creation of safety buffers instead of improving the poor supply chain performance. The problem with 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. Giunipero and Eltantawy (2003) anticipate that future supply professionals must direct the attention toward the uncertainty caused by risks in the company's 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 the role of a supply-chain professional becomes more strategic in the future (Giunipero et al., 2003). One concept that brings needed 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 of the holistically needed scheduling from 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 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. In figure 4 the temporary storage concept is induced into a transport network model.

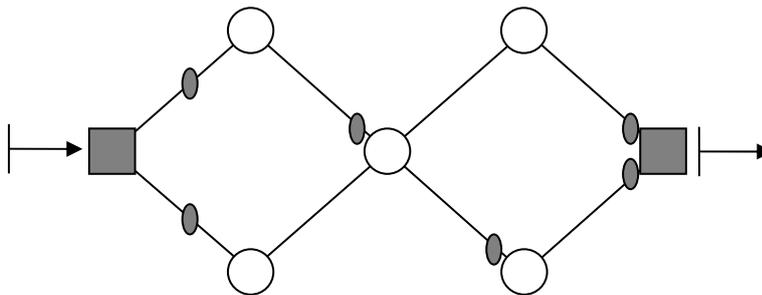


Figure 4: Transport network with resting-places

The terminal-close 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 factory's internal activity. Therefore 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 security of the material forwarding activity of the transport network contributes to reducing both the overall risk and the uncertainty of the supply chain. This is basically 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 inbound logistics risk. The consignor 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 inbound delivery window. This is illustrated in figure 5.

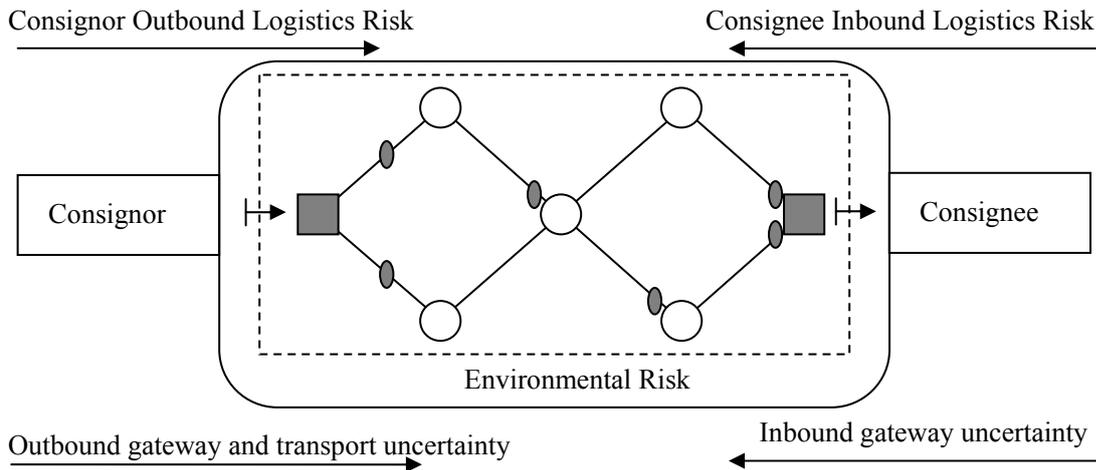


Figure 5: Risks and uncertainty in the transport network

The cause why a transport does not deliver within the scheduled time-window can be either deliberate or unintentional. The unintentional one is a process failure while the deliberate one is caused by antagonistic threats, normally called criminal activities. The need from the supply chain for a scheduling of all transport activities also provides crime opportunities according to Cohen and Felson's (1979) theory of routine activities perspective. This theory is a strong theoretical foundation to understand crime and opportunities for crime. The routine activities perspective argues that normal movement and other activities of both the potential perpetrators and their targets play a significant role in a potential crime and the prior opportunity for it. Crime opportunity is a cornerstone in all criminal behaviour, but opportunity alone does not lead to a crime (Felson et al., 1998). Perpetrators evaluate the situation or the opportunity by using external and internal variables and then decide how they best proceed. The reduction of uncertainty and risks caused by antagonistic activities inside the supply chain is called transport security or freight security.

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, 2006). 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. Especially 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. At present this cooperation is not widely developed (ECMT, 2001). Further there are different barriers in the business like the following: Underestimated risks from the haulers' side; different standard in technologies; insurance companies do not support by giving premium reductions; technical standards do not yet exist (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 police 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 organisation TAPA tries through its two different certification programs, Freight Security Standards (FSR) and Trucking Security Requirements (TSR), to improve 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 webpage). The TSR, on the other hand, addresses only security issues in road transport using lorries and is certified by self-assessment. 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 complement program to the FSR (TAPA, webpage). A transport network that is certified by TAPA can be illustrated as in figure 5.

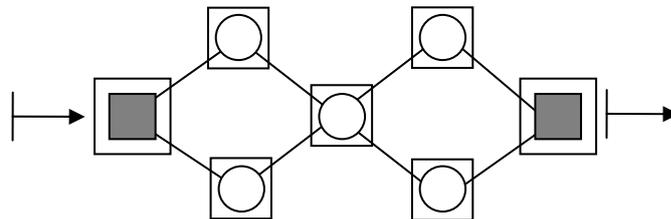


Figure 5: Security in the transport network

In transport security it is important to take an intermodal approach to avoid unwanted competition disadvantage 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 an intermodal transport the first and last part of the freight are conducted by road transport 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 the risk and uncertainty for the supply chain, without adding theft risk in the transport network

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 can be simplified by referring to both external and internal demands in the supply chain. The supply chain internal demands can be illustrated by scheduling of the transport and the delivery time by extended use of just-in-time delivery. The supply chain external demand comes 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 terminal-close temporary storage places reduce uncertainty by making it smoother to schedule all delivery according to demands and needs in the receiving terminal. This also reduces the risks from supplier. The external authorities' demands 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 be in the future six times more predictable by the location instead of perpetrator. Therefore is it 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 therefore to be securer 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.

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. This reduction of risk and uncertainty generated within the transport network can be achieved with additional and exact scheduling of delivery. The use of slot-times, similar to the air traffic network, is one way to achieve just that scheduling. Another reductive measurement is the use of secure parking spaces, whenever a resource needs to make a temporary stop. The third and commonly most suggested reductive measure is to utilize different types of tracking and tracing system. All these reductive measures could work together and as a combined toolbox they can contribute to reducing risk and uncertainty in the supply chain.

References

Beck, A. and Bilby, C. and Chapman, P. (2003), "Tackling shrinkage in the fast moving consumer goods supply chain: Developing a methodology". *Security journal*, Vol. 16, No. 2, pp 61-75, Perpetuity Press.

Chapman, P. and Christopher, M. and Juttner, U. and Peck, H. (2002), "Identifying and Managing Supply Chain Vulnerability". *Logistics & transport focus*, Vol.4, No. 4, pp. 59-64.

Christopher, M. (1998), *Logistics and supply chain management*. Prentice Hall London.

Christopher, M. and Lee, H. (2004), "Mitigating supply chain risk through improved confidence". *International journal of physical distribution and logistics management*, Vol. 34 No. 5, pp. 388-96.

Christopher, M. and Peck H. (2004), "Building the resilient supply chain". *International journal of logistics management*, Vol. 15 No. 2, pp. 1-13.

Cohen, L. E. and Felson, M. (1979), "Social change and crime rate trends: A routine activity approach". *American sociological review*, No 44.

Das, A and Handfield, R (1997) "Just-in-time and logistics in global sourcing: an empirical study". *International journal of physical distribution and logistics management*, Vol. 27 No. 3/4, 1997,

Disney S. and Towill D. (2003), "Vendor-managed inventory and bullwhip reduction in a two-level supply chain". *International journal of operations & production management*, Vol. 23, No. 6, pp. 625-651.

EC (2003), "Freight Transport Security". *Consultation paper*, European Commission, Brussels.

ECMT (2001), *Improving security for road freight vehicles*. Paris: OECD Publication Service

ECR (2001), "Shrinkage: introducing a collaborative approach to reducing stock loss in the supply chain". ECR Europe

Ekwall, D. (2006), "Cargo theft in supply chains: Crime displacement in the transport network".

Felson, M. and Clarke, R.V. (1998), "Opportunity makes the thief: Practical Theory for crime prevention". Home office police and reducing crime unit: London

Giunipero, L. and Eltantawy, R. (2004), "Securing the upstream supply chain: a risk management approach". *International journal of physical distribution & logistics management*, Vol. 34, No. 9, pp. 698-713.

Hoekstra, S. and Romme, J. (1992), *Integrated Logistics Structures: Developing Customer Oriented Goods Flow*. McGraw-Hill, London.

Juttner, U. (2005), "Supply chain risk management: Understanding the business requirements from a practitioner perspective". *The international journal of logistics management*, Vol. 16 No. 1, pp. 120 – 141.

Lalwani, C.S and Disney, S. M. and Naim, M. M. (2006), "On assessing the sensitivity to uncertainty in distribution network design". *International journal of physical distribution & logistics management*, Vol. 36, No. 1, pp. 5-21.

Lambert, D. and Stock, J. (1993), *Strategic logistics management*. Richard D Irwin Inc, US.

Lambert, D. and Stock, J. and Ellram, L. (1998), *Fundamentals of Logistics Management*, International ed., McGraw-Hill Higher Education, London.

Lumsden, K. (2006), *Logistikens grunder*. Studentlitteratur, Lund (In Swedish)

Lumsden, K. and Dallari, F. and Ruggeri, R. (1999), "Improving the efficiency of the Hub and Spoke system for the SKF European distribution network". *International journal of physical distribution & logistics management*, Vol. 29 No. 1, pp. 50-64.

Manunta, G. (1999), "What is security?". *Security journal*, Vol. 12, No. 3, pp 57-66, Perpetuity Press.

Mason-Jones, R. and Towill, D.R. (1998), "Shrinking the supply chain uncertainty circle". *The Institute of Operations Management Control Magazine*, Vol. 24 No. 7, pp. 17-23.

McCullen, P. and Towill, D.R. (2002), "Diagnosis and reduction of bullwhip in supply chains". *International journal of supply chain management*, Vol. 7 No. 3, pp. 164-79.

Mitchell, T, (1923), "Competitive illusion as a cause of business cycles". *Quarterly journal of economics*, Vol. 38, pp. 631-52.

Nilsson, F. (2004), "Simplicity vs Complexity in the Logistics Discipline – A Paradigmatic Discourse". *NOFOMA*, Linköping.

Nilsson, F. (2006), "Logistics management in practice – towards theories of complex logistics". *The International journal of logistics management*, Vol. 17, No. 1, pp. 38-54.

von Oetinger, B. (2004), "A plea for uncertainty: Everybody complains about uncertainty, but it might be a good thing to have". *Journal of business strategy*, Vol. 25, No 1, pp. 57-59.

Peck, H. (2005), "Drivers of supply chain vulnerability: an integrated framework". *International journal of physical distribution and logistics management*, Vol. 35 No. 4, pp. 210-232.

Popper, K. (1959), *The logic of scientific discovery*. Routledge London.

Prater, E. and Biehl, M. and Smith, M. (2001), "International supply chain agility, Tradeoff between flexibility and uncertainty". *International journal of operations & production management*, Vol. 21, No. 5, pp. 823-839.

Prater, E. (2005), "A framework for understanding the interaction of uncertainty and information systems on supply chain". *International journal of physical distribution and logistics management*, Vol. 35, No. 7, pp. 524-539.

Sabath, R. (1998), "Volatile demand calls for quick response: The integrated supply chain". *International journal of physical distribution & logistics management*, Vol. 28, No. 9, pp. 698-703.

Sherman, L.W. (1995), "Hot Spots of Crime and Criminal Careers of Places". In Eck, J.E. and Weisburd, D. (ed.), *Crime and place*, Vol. 4 pp. 35-52. Monsey, New York: Criminal Justice Press.

Sheffi, Y. (2001), "Supply chain management under the threat of international terrorism". *International journal of logistics management*, Vol. 12, No. 2, pp. 1-11.

Stefansson, G (2004), *Collaborative Logistics Management*. Chalmers, Gothenburg.

Svensson, G. (2002), "A conceptual framework of vulnerability in firms' inbound and outbound logistics flows", *International journal of physical distribution & logistics management*, Vol. 32, No. 2, pp. 110-34.

Svensson, G. (2003), "The principle of balance between companies' inventories and disturbances in logistics flows". *International journal of physical distribution & logistics management*, Vol. 33, No. 9, pp. 765-784.

TAPA, Technology Assets Protection Association, <http://www.tapaemea.com/engl/index.html>

Towill, D. (2005), "The impact of business policy on bullwhip induced risk in supply chain management". *International journal of physical distribution & logistics management*, Vol. 35, No. 8, pp. 555-575.

Wang, J. and Roush, M. (2000), *What every engineer should know about risk engineering and management*. Marcel Dekker inc. New York.

White, D. (1995), "Application of systems thinking to risk management: a review of the literature". *Management decision*, Vol. 33, No. 10, pp. 35-45.

Wikner, J. and Rudberg, M. (2005), "Integrating production and engineering perspectives on the customer order decoupling point". *International journal of operations & production management*, Vol. 25, No. 7, pp. 623-641.

Wilding, R. (1998), "The supply chain complexity triangle: uncertainty generation in the supply chain". *International journal of physical distribution and logistics management*, Vol. 28, No. 8, pp. 599-616.

Zinn, W. and Levy, M. and Bowersox, D.J. (1989), "Measuring the effect of inventory centralization/decentralization on aggregate safety stock: 'the square root law' revisited". *Journal of business logistics*, Vol. 10 No. 1, pp. 1-13.

Zsidisin, G. and Panelli, A. and Upton, R. (2000), "Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study". *Supply chain management: an international journal*, Vol. 5 No. 4, p. 171.