Chapter 8

Supply Chain Security – Threats and Solutions

Daniel Ekwall

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/48365

1. Introduction

In recent years, the cargo transport process has improved mainly in the areas of logistics efficiency and documentation handling. The World Trade Centre terror attack in 2001 changed the world and with it the conditions for logistics world-wide. The logistics consequences were according to[1]: *It is instructive to note that these disruptions were not caused by the attack itself, but rather by the government's response to the attack: closing borders, shutting down air traffic and evacuating buildings throughout the country*. The aftermath to the attack brought needed attention to the vulnerability of modern supply chains. Supply chain vulnerability reflects sensitivity of the supply chain to disruption [2]. 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 objective of Supply chain security is to prevent antagonistic threats from affecting the supply chain performance. Antagonistic threats and other risks and uncertainties are demarcated by three key words: deliberate (caused), illegal (defined by law), and hostile (negative impact for transport network activities) [3].

This chapter presents first the major antagonistic threats to the supply chain and secondly how these threats should be prevented. This leads to the current development of different supply chain security programs.

2. Supply chain and the transport network

[4] defines the supply chain as, "*The network of organisations that are involved through upstream and downstream relationships in the different processes and activities that produce value in the form of products and services in the hands of the ultimate customer*". These processes can be in different companies or in the same company. The different building blocks in a supply chain can, literally, be located throughout the world and connected through the use of a transport network. The transport network is designed to use economy of scale when moving products

from consignor to consignee in a supply chain, through nodes and links. This means the transport network only physically integrates the supply chain with the fulfilment of its transport demands [5]. Therefore, several different supply chains can be present at the same time and the same place in the transport network. This indicates that the relationship between supply chains and transport activities would be better described with complexity theory, especially if the interactions between components are the object of the research [3].

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 [6]. A logistics system consists of links and nodes, where nodes are geographically fixed points such as factories and terminals, while the links are the elements connecting the nodes, i.e., the modes of conveyance. The flow of materials is the first level of the system, because it is the reason for the system's existence. Moving material from one place to another requires a flow of movable resources such as Lorries, trains, airplanes, and ships. These movable resources need infrastructure like roads, harbours, airports, and terminals [7, 8].

The complexity in logistics can be explained by displaying the four flows always involved in logistics activities. The flows of material and resources are mentioned already. These two flows represent the "physical" part of logistics, but the other two flows, monetary stream and flow of information, are just as necessary to make the system work [6]. The four flows of logistics need geographical fixed constructions and infrastructure to fulfil the scope of logistics. Some of the infrastructure is owned and used exclusively by one company while some is co-owned or owned by governments. The four flows of logistics and the necessary infrastructure are the five needs for logistics fulfilment [9].

The cargo thief aims to remove goods from the goods flow by attacking the movement of resources and/or the infrastructure it uses. A potential perpetrator can also utilize the information flow in order to better plan the theft of goods or commit a fraud which targets the flow of capital. This paper uses primary the three elements, flow of goods, movement of resources and infrastructure of the five needs for logistics fulfilments. The frame of reference uses the routine activity theory from criminology to explain the interaction between the transport network and potential perpetrators, where the theft opportunity is determent by each unique configuration of the five needs for logistics fulfilments and then exploited by a potential perpetrator.

3. Threats to supply chains

3.1. Usage of official macro statistics

The usage of general statistics (mainly different types of criminal statistics) can provide a hint about the general criminal threat in a country or local area [9]. This fact is well known. Sometime is the relationship between reported crimes and public fear of crime direct whiles other times more indirect. Thus, it is possible that inverts that relationship and use macro level statistics in order to hint criminal hotspots in general. Important to remember is that this only provides a general hint about criminal threats and this clearly limited the

possibility to draw far-fetched conclusions unless more detailed data is added. A good indicator for criminal threats and common distrust in the society is level of corruption in a country [10]. The higher level of corruption, the higher is the distrust in the society and this may lead to a lower will to report crimes to the police. This is only a weak indicator.

A good indicator of the violence present in a society is the number of homicides per 100 000 citizens (lower number means safer). The average homicides rate 2007 in EU which is 1.4 in general but increases to 1.9 in capital cities [11]. This indicates that the country sides are safer than bigger cities, and the long term trend is a lower average homicides rate, which means a safer society (relatively). Other good indicators of criminal threats are the reported total number of crimes as well as the reported number of thefts and robberies. Risk rating (both relative and absolute) are good indicators on more transport related crimes. It is important to remember that each country may (are likely to) have different definition of crimes and guidelines for data collection [9].

The general criminal trend in EU is that crime is declining from the pike around 1995. According to [11] have their being an increase in reported crimes types violent crime (up 3%), drug trafficking and robbery (both up 1%) in the period 1998-2007. During the same period has seen a decrease in motor vehicle crimes (down 7%) and domestic burglary (down 3%). There seems to be a time difference between countries in the trend but nevertheless the declining in reported crimes and even criminal patterns are surprisingly similar between member states [12]. The reason for this decline is according [12] the "*changing demographics, among other factors, have played a causal role in the decreases in crime across the Western world. Since the bulk of common crimes are committed by young males".* There is also a suggestion that the better policing and/or more severe sentencing contributes to the declining criminal trend [12]. The different official statistics supports these conclusions.

3.2. Shrinkage and theft

The term inventory shrinkage is the loss of products between the point of manufacturing or purchase from supplier and the point of sale. According to [13], the average shrinkage rate is 1,8 percent of total annual sales. This means a total loss of $33,21 billion annually in the U.S. The report points out four major sources of shrinkage: employee theft, shoplifting, administrative error, and vendor fraud. Therefore, three of four sources for shrinkage are criminal actions. The losses in the European fast moving consumer goods are for 26 percent in manufacturing, 8 percent in distribution, and 66 percent in retail [14]. Shrinkage during distribution/transport is approximately 0,14 percent of annual sales for all types of products. According [15] is the worldwide loss ratio as 0,025 percent of the total revenue ($307 billion revenue and $77 million in losses). Benchmark participant loss rates varied from 0,0038 percent to 0,25 percent of total revenue. The three different reports [13, 14, 15] indicate that the annual shrinkage during distribution/transport would be 0,025 percent to 0,14 percent of annual sales. This loss ratio is compared with the loss ratio for retailers (1,75 percent) and manufacturers (0,56 percent) [14].

There is a significant problem with the theft of cargo worldwide. It is estimated that theft represents a loss of at least US$10 billion per year in the United States and US$30 billion worldwide [16]. The value of cargo theft for the European Union is estimated to be €8.2 billion annually, an average value of € 6.72 per trip [17]. Gathering accurate numbers for cargo theft losses is difficult or impossible in many cases, due to limited reporting by the transport industry and the lack of a national law enforcement system requiring reporting and tracking uniformity [18]. Despite these figures, cargo theft generally has a low priority status in most countries and is often perceived largely as the cost of doing business.

A problem related to cargo theft is the theft of vehicles and the lorry-driver's private property. There are many reasons behind a truck theft, but they can be described basically with three main characteristics - value, cargo carrying ability, and valuable documents [3]. *The first characteristic,* value, represents the truck's value as all objects and can be sold and exchanged for money. *The second characteristic, carrying ability,* refers to the general propose of a truck. The vehicle and its load were targeted in 63 percent of the attacks [19]. The truck can be stolen with the current load where the goods are the desirable object and the truck is only the simplest method to move the goods to a warehouse or to another truck for further movement. A truck also can be stolen for other criminal activities.

The third characteristic of theft problems toward freight is the attack for the lorry-driver's private property or other types of valuable documents such as credit cards, mobile phones, and digital cameras stored in the truck during transport. According [19], 17 percent of all drivers suffered an attack during the past five years, 30 percent were attacked more than once. Of all drivers attacked, 21 percent reported they were physically assaulted during the attack [19]. This type of attack represents a considerable amount of the total, but nothing was stolen in 38 percent of attacks against trucks [20]. However, even if nothing was stolen it was still a crime against a part of the transport network and therefore shall be seen as an antagonistic threat. 70 percent of attacks against road transports occur between 22:00 in the evening and 06:00 in the morning [19]. Therefore, it is possible to state that time of day plays an important role in antagonistic threats. According [19], the direct cost for an attack is approximately €25000 per attack, including theft of vehicles, load and the driver's personal belongings.

Regardless of which of the three characteristics of theft problems the motivated perpetrator uses, there is a number of commonly defined modus operandi or methods to attack trucks. These different modus operandi are used differently depending on where the attack is executed. The different locations are described in terms of different steps in a road transport from consignor to consignee, which starts with loading the goods and ends when unloading them. Eurowatch has developed a threat/risk matrix based on the data on cargo theft in road transports over a seven-year period [23]. The matrix presented in Table 1 maps modus operandi and location of attacks against each other.

A quick analysis of the matrix points out some obvious relationships. The method *fake accident* is best suited to deceive a truck driver to stop during driving and then conversion to a hijack. The same course of events can be created with the use of *fake police* tactics. The

threat/risk matrix points out the most dangerous location to be *near end location* or at *insecure parking* depending on which modus operandi is considered most threatening.

	Hijack	Robbery	Theft from vehicle	Theft of vehicle	Fake police	Fake accident	Deception
Load point	2	3	2	3	1	1	4
Driving	4	1	1	1	4	4	2
Insecure parking	2	4	4	4	3	1	2
Secure parking	2	2	3	3	1	1	2
Near end Location	4	3	3	4	3	1	3
Unload point	2	3	2	3	1	1	4

Table 1. Threat/risk matrix, road transport using Eurowatch data 2002-2009, 4 represents the highest risk [23]

The greatest source of risk for businesses is trusted insiders [21]. Some authors consider insiders to be involved in approximately 60 percent of all losses [22]. According to [23] is 65 percent of all "whole load losses" related to the use of inside information. Others claim there are no reliable figures [24]. This is interesting when considering the fact that most countermeasures are implemented to reduce external theft [25]. An internal perpetrator acts not randomly or in an unstructured way, but more as a response to social and environmental factors present in the work environment [22]. According [26] is the complexity around insiders and drivers expressed: *"Some estimates indicate a high level of driver involvement, but drivers are possibly the weakest link in the security of the supply chain. They are also the first line of defence and there is a need to train and educate them on cargo crime and personal safety issues whilst on the road."* This leads to that the potential perpetrator both can be external to and internally involved in the supply and/or the transport chain.

3.3. Terrorism

The word "terror" is a Latin word meaning "to frighten." Consequently, a terrorist is a person that intends to frighten others through fear. The term terrorist/terrorism is itself controversial because its key signature is political and it has been used by states to illegitimatize political opponents. This leads to a vindication of the state's own use of terror against its opponents [27]. The lack of a universal definition of consequence of this is best explained with the cynical comment "*that one state's terrorist is another state's freedom fighter*". Regardless, terrorism is definition by [28] as, "*Terrorism is not an ideology or movement, but a tactic or a method for attaining political goals.* Terrorism is one of the major obstacles for meaningful international countermeasures.

The World Trade Centre terror attack in 2001 changed the world and the conditions for logistics worldwide. The aftermath of the terrorist attacks clearly indicated that logistics operations will suffer consequences of an attack. [29] state that, "*over the longer term, there is a question of whether the attacks can have a negative impact on productivity by raising the costs of transactions through increased security measures, higher insurance premiums, and the increased costs of financial and other counterterrorism regulations*". The motivation for the majority of terrorist attacks is because the perpetrator intends to influence and alter the current balance of power in a certain direction [30]. Both the current balance of power and the potential effects on it may only be understood within the perpetrator's own mind. Therefore, the non-economically driven antagonistic threat is more nuanced, uncertain, and harder to predict that other types of antagonistic threats. According to [31] the fear for terrorist attacks is an extreme form of perceived risk. The definition of terrorism influences the difficulty to present valid statistics for the category, because one source may classify an incident as a terrorist act while another considers it to be a "regular" crime. According [28] is the official reported number of terrorism attack in EU declining (581 attacks in 2007 and 294 attacks in 2009) and the major threat (in numbers) comes for separatist movements (Basque and Corsican) whiles Islamist terrorism is still perceived as the biggest threat.

The modern or new thing with terrorism is not the use of violence to influence and alter the current balance of power in a certain direction. According to [32] is: *"Terrorism in all its forms, by its very nature, an asymmetrical response to superior force, and terrorist have always used their capabilities as force multipliers – usually through the exploitation of terror. The generation of fear, in effect the use of purposeful violence as a form of psychological warfare can now be carried much further, enhanced by the modern media and the proliferation of mass media as much as by the proliferation of weapons".* The new thing with terrorism is therefore more related to development in media technologies than to vulnerabilities in supply chains. Nevertheless, terrorism is a special form of antagonistic threat that needs to be managed, in one way or another.

Reviewing official terrorist statistics from one global source (MIPT Terrorism Knowledge Base) leads to the following transport related conclusions:

- Transport activities represent 4% of the targets in 2006 and 5% in 2007.
- The main modus operandi for attacks is armed attack (38% 2006 and 31% 2007) and bombing (51% 2006 and 54% 2007).
- The main area for terrorist attacks are Middle East/Persian Gulf (68% 2006), and Asia (24% 2006).

The terrorists prefer to use bombs and armed attacks because 80-90 percent of all attacks used these tactics. The targets are rarely transports but more in form of police and other governmental or religious institutions (~53% of the attack 2006). The interesting feature is related to the geographic side of terrorism, because the terrorist threat is mainly linked to local/country/regional contexts.

The official statistics for terrorist attacks indicates that, in order to understand terrorists, it is better to focus on possible attacks instead of probability for attacks. In accordance with this, there is no objective [33] way to determine who is a terrorist and who is not. It has all to do with the context to the terrorist threat. This follows the same logic when terrorism is presented as black swan problem [34]. Nevertheless direct and indirect effects from a terrorist attack or threat will affect the global flow of goods and thereby, to different extent, the global economy.

3.4. Smuggling of goods

The primary target of illegal goods is the black market. The black market consists of places and situations where products with doubtful or no legality are traded for money. This market is subject to the same forces of supply and demand as legal ones. Buyers of these illegal products are everywhere. Statistical reports show that counterfeited and pirated items amounted to $176 billion in Europe in 2007 [35]. According to [36], in 2006, nearly 3 million pharmaceutical products were found to be counterfeit. Product smuggling does not necessarily mean that the product is illegal everywhere. What is legal in one country can be illegal in another, which creates the possibility that the actors in smuggling can be legal companies that are trying to access a market that is prohibited for them. An example of this is Western companies that smuggled products into former communist countries during the Cold War era.

The supply of a typical black market (both authorities and customers knows that the product is illegal) can be illustrated with the illegal smuggling of cocaine to USA. The illegal drug supply chains come mainly from South America. This depends on that the raw material, coca leaf, is grown there. The smugglers use land, sea, and air routes to get past US authorities. The whole distribution of cocaine is controlled by Colombian-based organized crime, but in recent years it has started to cooperate with Mexican criminals to streamline the logistics and share the risks. The Colombians have organized their operations in a business-like manner, creating cells for special purposes like warehousing or transport [37]. According [38], the illegal drug markets are best understood as having high adaptation and great resilience to always supply their products to the end user. This resilience and adaptive ability is clearly found in the logistics system setup and can be understood and explained with the concept of risk for detection presented in this paper.

The supply of a typical gray market (only authorities know that the product is illegal) can be illustrated with the illegal smuggling of counterfeited products. The gray market involves the diversion of goods from legitimate supply chains [39]. The only distinction is the risk for discovery from the authorities or the company whose products are copied. This diversity leads to a different design of the supply chain. The location of the production facilities is subject to the risk of discovery. Normally, counterfeited production units are placed where the risk for detection is low combined with the normal business problem as different types of costs and quality aspects. A counterfeited supply chain uses

the freight routes and port activities in the same way as legal supply chain does. Among the receiver countries, Europe and the US are favorites, just as Africa is the favorite for transit activities. Confiscated products that have not been produced in Africa, like jewelry and CDs, show this, because the African market does not have the ability, in general, to buy that type of product. Countries in Central and South America act like magnets for counterfeited products. Purchases of counterfeited goods to launder money occur in larger numbers there than anywhere else in the world [40]. Large stocks of illegitimate products are easily shipped from parts of South America to Central America, where they are big consumers of that type of product. Organized crime also uses Central America as the base for shipments of illegitimate goods to North America. The situation in Europe makes it the most lucrative market for counterfeited products. The types of confiscated goods at the external borders of the EU are different from other places in the world. This indicates that the dealers of counterfeited products adjust products to each market's special condition. They look at the fashion, culture, and buying habits of individual countries [40].

Both types of Illegal supply chains use the international flow of containers to transport their products all over the world, regardless if the product is counterfeited or an illegal drug. Criminals try to delude customs' watchfulness by "breaking" their way through from the area of production to the area of supply, and avoiding direct paths that are well known to the authorities.

A problem linked to smuggling is the manufacturing of products without intellectual rights, or the production of counterfeited goods. Everything that has been produced can be reproduced by someone else. In order to bring counterfeited products from the production site to the end user, they may have to cross several national boundaries as well as intellectual property legislation. The counterfeiting business evolves constantly within current trends and technologies. The production and distribution of illegal products is performed under the risk for detection and this diversity leads to a different design of the supply chain [41]. The location of the production facilities is subject to the risk of discovery. Normally, illegal production units are placed where the risk for detection is low, in line with the normal legal business problem of where to produce according to different types of costs and quality aspects. Then, the illegal products are distributed by trade routes and port activities in the same way as legal products [42]. The pollution of illegal products in the legal transport network is a serious problem. The most common countermeasure against smuggling is the inspection of cargo carriers when they cross a national border. The mere existence of these inspections creates disturbances in the transport network, even if no illegal product is discovered.

The counterfeiting business evolves constantly within current trends and technologies. The illegal products are then distributed by trade routes and port activities in the same way as legal products [42]. According [43], the discourse on the gray market is filled with the idea of a criminal underworld in order to separate it from the legal/normal upper-world. In reality is it very difficult to establish the underworld/upper-world image. The legal

companies naturally are not pleased with the competition from black market actors. They may not be pleased with legal competition either, but that is another question. Striving for better business deals and the globalization trend that started centuries ago led to an embedment of illegal actions within legal markets [42]. This implies that the old black markets have been integrated with legal transactions, and today's markets contain every shade of gray when referring to the legality of the markets as a whole [42]. Legal businesses are concerned especially with the problems of counterfeit branded products and the theft of their own products. To increase the efficiency of detecting counterfeited products, legal businesses use cutting-edge technology and security actions [97].

3.5. Piracy

The modern types of pirates do not act officially of any specific courtiers' order but research has indicated relationship between piracy and weakness of central governances [44]. In essence is piracy an international crime against all states and the perpetrators can be brought to justice in all everywhere [45]. In recent years has the threat from piracy against sea shipment (direct threat) and also against the different supply chains utilizing sea shipment (indirect threat) received increasing attention [44, 46, 47, 48]. The real increasing threat from pirates, primary at the horn of Africa [45, 47], has resulted into both a changes in shipping routes (Sullivan, 2010) and also a naval response from several countries [46] that are depended on a smooth passage of cargo carrying ships. According [49], was there 489 attacks last year (2010) and over a twelve year period was there about 347 attacks/year globally [43]. Piracy is an increasing problem, especially near Somalia [48]. The pirates are changing their tactics and targets to use more sophisticated weaponry and apply more advanced techniques, all in order to improve their own success ratio. Table 2 presents the current trends and patterns in piracy.

Year	**Number of acts**	**Lives lost**	**Wounded crew**	**Missing crew**	**Crew hostage/ Kidnapped**	**Crew assaulted**	**Ships hijacked**	**Ships missing**
2006	254	17	23	0	224	225	10	0
2007	310	22	75	57	223	39	18	0
2008	330	6	22	38	773	21	47	1
2009	406	8	57	9	746	2	56	2
2010	489	1	27	0	1027	30	57	12

Table 2. Trends and numbers in piracy 2006-2010 [48]

As stated in table 2, piracy is an increasing threat and especially alarming is the increasing use of violent and kidnapping of crew members. According to [48], piracy cost the maritime industry between 7 - 12 billion dollars a year. In addition to this shall also the cost for rerouting to avoid pirate infested waters, ransom payments and support from various organizations be added.

4. Preventing the threats - solutions

4.1. Interdisciplinary research mixing criminology into logistics

According to several authors [50, 51, 52], criminology is interdisciplinary research of the history and future of crimes, and this paper follows this tradition by using theories from criminology to strengthen the field of logistics. This mix of theories also challenges the predominant research approach in logistics related to tangible artefacts [53], and human intervention or influence to a smaller extent [54]. The reason for this approach is that violation of law is considered a human attribute. Criminology distinguishes three elements of a crime that are present in all sorts of crime ranging from occasional violence to advance and complex economic crimes [55, 56, 57]. The elements are:

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

These three different elements can be described as:

Motivated perpetrator: The perpetrator is an individual that, based on the outcome of the own decision process, commits a certain action or prepares for a certain action that is prohibited by locality or country of international law. The perpetrator can be modelled with two different categories depending on how decisions are made by each individual, namely rational choice theory (also known as the economical man theory) or determinism [54, 58]. It is commonly agreed that different crimes demand various mixtures of rational choice and determinism from the perpetrator's side, where crimes of passion (sexual crime, etc.) are considered more deterministic than property crimes (economic crime, etc.), which are more rational [59]. Thus, therefore can the general description of human behaviour be described as acting rational on the margin or limited (by circumstance, choice or mixture of both) rational choice [60, 61].

Object: The desirable outcomes or objects for the motivated perpetrator differ greatly depending on the motivated perpetrator's decision process. Normally is it suitable to describe the object as the primary or direct reason for the action, but also as secondary or indirect reasons [56]. The primary objects can be shipped products, resources used, infrastructure, or even the media attention an attack will receive (terrorist attacks, action junkies etc.). It is in the relationship between object and motivated perpetrator that the categorisation of the antagonistic threat is found [3].

Lack of capable guardian: The preventive measures that can be induced to alter the motivated perpetrator's decision process are called security [62]. If the security measures are considered insufficient by the motivated perpetrator, then there is nothing to prevent the crime [56].

Most important to remember about the elements of crime is that it is first when all three elements comes together at the same time that a crime is possible. This means that if one of the three elements is missing than is crime impossible. Any combination of lack of security and target are normally referred to as a crime opportunity.

4.2. Opportunity to crime

Crime opportunity is a cornerstone of criminal behaviour. There are ten crime opportunity principles as follows [63]:

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

Some of these principles are self-explanatory and easy to understand. All of them are valid for every type of crime and therefore they are also valid for crimes committed against the transport network. The more interesting examples of these opportunities will be explained and described later in this thesis. The most important thing to remember about crime opportunity is that an opportunity alone does not explain why a crime occurs because a crime needs a motivated perpetrator and opportunity to occur [64]. The theory of crime opportunity also refers to the fourth principle of microeconomics [57] - *people respond to incentives* - and there the degree of necessary opportunity or incentive depends on the individual. The incentives could range from vindication to morality, ethics, altruism, or determinism [3, 64]. Altogether, this leads to that the relationship between threats (motivated perpetrator) and countermeasures (security) linked around a desirable outcome or object, are complex and contextual depended.

4.3. The two different outlooks on mankind in criminology

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

Modern criminology uses rational choice theory as the basis for research. Rational choice theory, also known as rational action theory, is a framework for describing and modeling social and economic behavior. This theory originates in the idea of the economic man in economic research, primarily microeconomics. This theoretical model is also central in modern political science and scientific fields such as sociology and philosophy. Rational choice theory assumes that individuals choose the best action according to the constraints, opportunities, functions, and abilities they face. Today, rational choice theory in microeconomics is defined best with the first four principles of microeconomics [58]. In short, the theory states that every presumed criminal is should be considered a rational person who makes decisions about potential crime from relationships between the benefits

of the crime and the troubles and risk it brings. By increasing the perceived trouble and/or risk, it is possible to reduce criminal activity with this perspective [55].

The opposite of rational choice is determinism. The idea is that the course of events depends completely on existing conditions. This approach refuses the idea of free will - everything is predetermined. In reality, every individual is a mixture of their ability to be influenced and the lawful. Among social scientists today, the idea of restricted free will is a common and useful insight. The cause of these restrictions can be found in the individual biological or psychological vulnerability, way of life, upbringing, social group, ethnic background, or society in which the individual lives, and how this affects his or her life with regard to their ethnic background, gender, and social position [55].

These opposing perspectives of the human being as either the master of his own life or as a victim of circumstance can be found in every aspect of criminology. This contrast affects not only how we see the causes of criminal behaviour, but is also important with respect to the social response to criminal behaviour [55]. According to [65], the current approach toward crime, punishment, and pardon is a good way to understand the surrounding society. It is commonly agreed that different crimes demand various mixtures of rational choice and determinism from the perpetrator's side, where crimes of passion (sexual crime, etc.) are considered more deterministic than property crimes (economic crime, etc.), which are more rational. That being said, the big difference appears when discussing the possible punishment for a certain crime. If an individual is responsible for his or her actions (rational choice), then the possible punishment will deter the crime; however, if the individual is a victim of circumstance (determinism), then it is useless to punish the individual. Therefore all crime prevention methods assume that an individual is responsible for his own actions and that he can perceive the consequences of those actions. The big question for the rational choice perspective is how each individual estimates the risk in a rational way. An individual that has received a formal or perceived punishment for an action previously should be less likely to commit that action again. The outcome of a formal punishment on the perception of risk is mixed [66] and each individual should be considered not rational, but to act rationally on the margin [3].

4.4. Criminal prosecution and punishment

This discussion of the two outlooks on mankind in criminology clearly demonstrates the need to add theories from criminology into logistics. Several logistics authors claim that the weak prosecution of criminals is one reason behind the increasing need for security [16, 67, 68]. In the context of the two outlooks on mankind in criminology, [16, 67, 68], state the threats against logistics activities is simply based on the rational choice theory, while authors in criminology [55, 63, 66, 72, 74] refer to an individual acting rationally on the margin which eliminates the deterring effect of potential punishment that [16, 67, 68] suggest. The deterrent effect that a punishment can have on a perpetrator not to commit a certain crime is very low, due to that the perpetrators do not plan to get captured. Therefore has the risk for detection a bigger deterrent effect that the potential punishment [41]. The

authors' [16, 67, 68] request for stronger prosecution of criminals can be seen as a way to understand the surrounding society in general [65]. Compare that to [69] who state that risk management and TQM systems are normally linked to a punishment and reward system for the users. The difference between legal prosecution achieved by a state and a punishment and reward system controlled by a company or similar organization is that legal prosecution involves a weaker relationship between action and consequence for the perpetrator.

4.5. Perpetrator, opportunity and security

The relationship between security and opportunity is the predominant understanding of security in different contexts. This depends on the premise that security only can deter or repel a motivated perpetrator from committing a crime by limiting the opportunities for a certain crime. The most important thing to remember with crime opportunities is that an opportunity alone does not explain why a crime occurs because a crime needs a motivated perpetrator and opportunity to occur [62]. Opportunity plays a role in causing crime, and these opportunities are highly specific, concentrated in time and place, and depend on everyday movements. These opportunities can be reduced and focused opportunity reduction can produce wider declines in crime. It is the theory behind security. The real problem occurs when an organisation's security capability is lower than the capability of the potential perpetrator. The driving force within each potential perpetrator can be vindication from morality, ethics, altruism, or determinism. Therefore, the relationship between security and opportunity must be understood from the viewpoint that the parties involved (stakeholders, actors, and humans) have different individual incentives to exploit opportunity that security needs to address. Consequently, security cannot be seen as only opportunity limiting but also as incentive limiting, making security a preventive factor on both sides of the opportunity (pre- and post-event).

Crime opportunities depend on routines or predictability within certain boundaries. This is the routine activity perspective in criminology and it argues that normal movement and other routine activities play a significant role in potential crime. The routine activity theory states that potential perpetrators may seek locations where their victims or targets are numerous, available, convenient, and/or vulnerable. [70] uses the illustration of "*how lions look for deer near their watering hole*" to explain the practical relevance of the routine activity perspective. Social disorganization in combination with the routine activity theory can provide a wider and better explanation of property crime.

4.6. Incident preventing

The security of freight transport was long under-developed, but since terminal security has improved, theft incidents have increased in the links between terminals [71]. This development is also valid from a supply chain perspective; while security in manufacturing facilities normally is focused and well-managed, the rest of the chain is without security [72]. Security during transport is necessary to prevent unwanted negative disruption in the flow of goods. Transport security means the interaction between physical obstructing

artifacts (locks, fences, Closed Circuit Television (CCTV) etc.) and the intervention of humans, with the aim of reducing theft, sabotage and other types of illegal activity. The technological development of the range and sophistication of anti-theft devices and after-theft systems is increasing rapidly [73]. There are different preventive methods that can be used to reduce the risk of a cargo theft incident, but the primary method is to use physical security countermeasures correctly (fences, locks, seals, guards etc). 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 and new employee reference checks [74].

The configuration of transport networks leads to the need for security measures in different forms, depending on the exact function and appearance of each nod and link. All different theft preventive methods used can be explained with the basic theory of situational crime prevention. The aim is to reduce factors specific to different types of crimes, locations and situations. 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 [75]. 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 [76]. 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. 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 [77]:

Increased perceived effort [78] – Motivation to commit a theft is reduced if the perpetrator believes the crime is too hard to commit. Preventive actions based on this idea can be categorized as physical separation of the potential perpetrator and the object of the theft. This can be accomplished through the use of access control and physical barriers (fences, locks, etc.).

Increased perceived risks [70] – If perpetrators think they will get away with a theft, it is more likely they will commit it. By increasing the risk for perpetrators they are less likely to commit a theft. This can be accomplished with surveillance systems, security personnel, and by increasing employee's security awareness.

Reducing anticipated rewards [70] – People are more likely to commit a theft if they can benefit from it. By making the target for the theft worthless or reducing its resale value it becomes less attractive for potential perpetrators. This can be accomplished by marking the goods with unique numbers or a product destruction device. Good examples of this principle are the safety cases used in transports of valuables and money and the ink tags used in fashion stores.

[71] added a fourth preventive principle based on rational choice theory:

Inducing guilt or shame – A theft is more likely to occur if it can be excused by appeal to reasons such as "the company can afford it" or "I've worked hard for the company but they

have not thanked me for it" [79]. This is a form of ethic relativity. Companies and organizations can affect this ethic relativity by using company rules, signs, and regulations that demonstrate the right moral values. When theft is seen as an additional wage benefit for employees, this preventive action has failed [24]. By appealing to people's morals and making it easy for them to do the right thing, it will be more difficult to make excuses [71].

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 [80]. Both of these criticisms are valid for the usage of situational crime prevention to hinder cargo theft. This may explain the over confidence in technology in order to prevent terrorism due to that terrorism is not a property crime and therefore has the use of technology an even lower impact on reducing the threat than for a cargo theft incident. The prevention of incidents are traditionally closely linked to the definition of security as a *show of force* which leads to that security work becomes symbolised with uniformed guards and normal police duties [81]. In order to include impact reduction in the term security is the second definition, *freedom from danger*, better to use. This definition embraces all things that allow the organization to act and carryout the business "free from danger". This is from this view point the supply chain security shall be understood.

4.7. Crime displacement

The theory of crime displacement says that crime prevention in one area may have unintentional consequences in other areas or situations. Therefore, crime prevention may not lead to an absolute reduction in crime. The theory of crime displacement is based on rational choice theory, with the following three assumptions about the potential perpetrator and target [69]:

Crime displacement assumes that crime is inelastic [82] - 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 [83]. Professional criminals are more inelastic while opportunistic criminals are more elastic [75].

The perpetrator has mobility [75] - Perpetrators have flexibility relative to time, place, method, and type of crime. In reality, perpetrators are limited in their mobility, adaptability, and flexibility relative to a particular crime, place, time, and method [76].

There exist unlimited numbers of alternative targets [84] - 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 [76].

The theory of crime displacement states that rational thinking perpetrators with crime mobility will alter their behaviour in response to crime prevention efforts [69]. Crime displacement will only occur when the alternative crime has a similar cost-benefit structure rationalised within the perpetrator's decision process [85]. Based on the ten principles of

theft opportunities presented earlier in this thesis and the configuration of the transport network, it is obvious that all opportunities cannot be eliminated, but they can be reduced by applying substantive preventive countermeasures. The object is to reduce crime opportunities which will lead to a change in potential theft situations. Therefore crime displacement is a valid theory [75].

Crime displacement can occur in several ways. [75] uses five types of displacement - crime, target, method, place, and time. [86] add another type of displacement, the perpetrator. The six types of displacement are explained below [65]:

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

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

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

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

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

Perpetrator: Transfer to another perpetrator
Ex: Preventing one offender can create an opportunity for another offender.

The theory of crime displacement does not explain why perpetrators commit a certain crime or why some crimes are more attractive than others. Furthermore, it does not explain the perpetrator's perceptions and reactions to changes in opportunities [76]. Crime displacement is one probable explanation of why criminal patterns change in a certain system. A practical statement about crime displacement is that *if perpetrators have the ability, mobility, and flexibility to exploit the weakest link in the chain, they will do so*. It is the perpetrator's ability to organize a successful crime and their relationship relative to the actors within the transport network that are the fundamental variables for categorizing perpetrators.

4.8. Logistics, risk management and criminology

The three terms security, risk management, and crime prevention often are considered similar and always work together [61, 74]. This idea suggests that security and risk management are good from an ethics point of view because they reduce crime; therefore, more or better security or risk management will reduce crime. The problem here is that crime is defined by a law according to the principle "no crime without a law" [54], while security or risk management has no philosophical attachment to law. Therefore, people on both sides of the law can have better security or risk management and that security and risk management are not necessary against crime.

Security for an individual or a group of individuals can, if unrestricted, jeopardise the security of others by threatening them or transferring threats to them. This type of discussion can be found with philosophers such as Hobbes and Mills. Unbounded or unrestricted individual security could threaten the authority of a state. This problem is demonstrated in the current debate about individual and private secure communication encryption, which some states want to make illegal unless they can break them. Taking this into account, a security problem may or may not be a legal problem. As a concept, security involves a protector or guardian and a threat against an asset or object [74]. This threat can be from either side of the law. To obtain the right security, it is vital to answer who is protecting what, from whom, in which situation, to what extent, and to what consequence [61]. Security can be seen as contextual risk management [3].

Contextual and statistical risk management approaches as crime prevention methods work in different ways and address different types of potential perpetrators. This demonstrates the difference in the philosophical views of contextual and statistical risk management. Statistical risk management needs a fairly predictable world, or at least a larger amount of trustworthy statistics. Since previous events or incidents are the basis of statistical risk management, it cannot deal effectively with a self-inflicted alteration of the threat pattern. Therefore, statistical risk management is effective in crime prevention if the potential perpetrators are limited to unsophisticated and indifferent methods based on opportunistic behaviour [87]. However, as potential perpetrators become more sophisticated and gain more capability, the accuracy of statistical prediction will reduce dramatically. Antagonistic perpetrators study the victim to discover routines and regularities and improve their skills with this knowledge (planning, technologies, and tactics) to maximize their likelihood for success [88]. 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 [75].

4.9. Transfer of the effect from antagonistic threats

The mitigation of antagonistic threats refers to strategies to transfer the economic impact to another organisation/company. The basic idea is that by transferring the risk to someone else through different types of contracts, it reduces personal risk substantially [89, 90]. The contractual agreements are divided into two different categories - insurance policies and non-insurance contractual agreements between two organisations. Good risk transfer strategy is composed normally of both types of risk transfer.

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

insurance buyer is the central issue, and in extension, also the potential reduction of a potential loss [3, 91].

Today special insurance policies exist for everything from cargo damage and machinery breakdown to terrorism, war, and general consequence liability. Typically, all insist on special events to be considered valid for a certain incident. Sometimes the terms are so specific that different types of insurance are valid depending on the cause of the incident. One of the best examples is the often-conflicting terms in terrorism contra war insurance. If there is a recognized government behind the incident, then war insurance is valid, but if the incident is caused by someone else, it is the terrorism insurance policy that covers the economic impact. This also depends on the different terms that each insurance company has in their product [3].

Transfer of risk by usage of business power: This risk transfer strategy is commonly used between contractual partners, but is rarely mentioned because it opposes the belief that everybody wants to collaborate fairly and for the greater good [92, 93, 94, 95]. The general idea of this risk transfer strategy is to use the business power of size, information advantage, or control over a critical asset [96, 97] so the business partner can obtain a share of the business risk as a part of the contractual agreement.

4.10. Supply chain security

The terrorist attacks at the World Trade Centre and Pentagon on September 11, 2001, brought attention to security in trade, for more reasons than just the attacks. Three factors can be outlined: first, the globalization of world trade depends on and is generated by the free flow of people, goods, and information; second, the increasing demands from businesses for efficient supply chain operations; and third, the increasing threats of terrorist attacks [98]. The last reason can be seen as an increase in perceived risk for terrorist attacks. This factor can define 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*" [83]. The only problem with this definition is that it does not address the origin of the threat or risk. The five sources of supply chain risks provide that. Supply chain security needs to adjust its policies, procedures, and technology to protect the supply chain from all five risk sources. The flip side of supply chain security is supply chain resilience, or a supply chain's ability to withstand and recover from an incident [83]. Supply chain risk should incorporate security and resilience, where resilience also must handle a near miss incident that affects the performance of the supply chain and from which it needs to recover.

Present supply chain security research outlines several changes for how security in a supply chain should be approached. First, supply chain security should incorporate not only theft prevention but also anti-terrorism measures. Second, the focus is now on global issues and

not just local or national issues [99]. Third, when conducting contingency planning, the concept of crisis management is to be included to obtain better resilience. Last, security is no longer an internal corporate question but rather an issue for all actors within the supply chain [83].

[100] suggest that methods and ideas from total quality management can be used successfully to increase supply chain security. The main idea is the lesson from quality management that sample inspection is expensive and useless at the end of the production line. Just like in quality management, supply chain security becomes more effective and less expensive by implementing the right management approach, technology, and re-engineering operational processes. [85] state that security should be integrated throughout the entire supply chain to be successful at a reasonable price. This opinion is supported by several other authors [74, 83, 101, 102, 103].

4.11. Supply chain security programs

Several new security programmes were launched in the aftermath of the World Trade Centre terrorist attack to protect international cargo flow from being abused for criminal (primarily terrorist) intentions without compromising supply chain efficiency. The U.S. Customs Office launched several programmes such as the Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI), the 24-hour rule, etc. These security programmes address different aspects of supply chain security and target different parts of a transport chain. The link between these security programmes is that they involve all parties or stakeholders in supply chain security [104]. The effects from these programs both in order to handle security threats and their impact on different logistics processes have been addressed in a few papers [105, 106, 107, 108, 109]. [110] states that the C-TPAT certification will probably have a negative impact, mostly on small enterprises whiles large firms instead may have the possibility to trade-off the security costs with benefits related to supply chain transparency. [111] demonstrates the economical and competitive advantages for large and small shippers becoming FAST-approved (Free And Secure Trade). The acquisition of the FAST status may provide shippers with faster trans-border operations and consequently a substantial advantage on the export market [96]. [112] emphasize that efficiency and security in supply chains are closely related to each others, since higher security may reduce Customs delays. The relationship between security, efficiency and custom activities is clearly found in the AEO-program.

Other types of security programmes existed before the attacks on the World Trade Centre. These programmes were designed primarily to address theft problems within the transport business (TAPA FSR and TSR, etc.) [113]. The big difference between security programmes before and after the terrorist attacks is that afterwards, authorities (mainly U.S.) took the lead in developing and implementing these programmes. Before September 11, 2001, security was something the business itself handled. The implementation of these programmes has so far mainly occurred in the old western countries in North America and in Europe.

Other types of security programmes existed before the attacks on the World Trade Centre. These programmes were designed primarily to address theft problems within the transport business. The big difference between security programmes before and after the terrorist attacks is that afterwards, authorities (mainly U.S.) took the lead in developing and implementing these programmes. Before September 11, 2001, security was something the business itself handled. The implementation of these programmes has so far mainly occurred in the old western countries in North America and in Europe.

The cost for implementing these programs alters the current collaboration models with regards to risk and profit sharing within the supply chain. The risks for antagonist threats are depended on the local environment. This shall be compared with that the security programs advocates one to three different security levels which shall solve the problem. This leads to that the security level is adjusted towards the security programs instead of the local threat. This may lead to that the security cost is higher than needed but a standardisation within the supply/transport chain in security may result in better collaboration. The political reasons behind the different supply chain security programs is most likely the fear for terrorist attacks which according to [32] depends more on the *proliferation of mass media* than development of new weapons. This is the context to understand the content and effects from fear of terrorist against international trade. Nevertheless the supply chain security programs provides collateral benefits like better product control, lesser shrinkage and better incident prevention by reducing threat opportunities.

The compliance with these different logistics security programs are based on different reasons. The compliance with business logistics security programs (like TAPA:s) are based on customer requirements. This depends on the simple fact that these programs are focusing on theft prevention. The governmental logistics security programs like AEO, C-TPAT, CSI etc. are on other hand more focusing on preventing terrorist activities. These programs normally also contains some kind of disadvantage for the own organisation if not compliance. Therefore are the governmental logistics security programs entail with a higher likelihood of compliance due to that need for compliance are not based on a risk assessment about the potential causes and impacts for antagonistic threats but on a general business assessment. For legal businesses, the AEO, C-TPAT, etc., are both a global supply chain headache and a business opportunity, depending on the risk for theft and counterfeiting for that company [114]. Irrespective of the difference in compliance reasons, the governmental logistics security programs may result in collateral benefits like lower cost for theft and better working conditions for the employees but there are still to be demonstrated that the terrorism preventing logistics security programs actually reduces the risk for non-economical-driven antagonistic threats because it's their primer reason for existing.

5. Conclusions

First, [1] clearly points out the effects of the WTC terrorist attacks on the global flow of goods. The effect may be indirect, but it was devastating. This event along with non-

antagonistic events such as Hurricane Katrina and other natural disasters demonstrated their power to disrupt or cause uncertainty in supply chains. Second, terrorism conducts fund raising through criminal activities, which leads to that terrorism represents all antagonistic threats. Third, the tools and strategies for handling antagonistic threats are partly governmental (police and justice system) and partly consequence handling (insurance businesses, conventions and business contingency).

For terrorist threats, it is useful to refer to transferred and perceived threatening pictures [31]. The perceived or actual marketing strategies which link a company or organisation with certain values/states/advocates will affect the risks for terrorist threats to the organisation/business/market position. The key issue in this conclusion is that the perceived relationship between a company/organisation and values/states/advocates is made by the potential terrorist. Therefore is it important for a holistic threats assessment to include and consider these different relationships between an organisation and different values/states/advocates with regard to direct and more important indirect connections.

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

The vulnerability of the supply chain is transmitted to the transport network. This depends on the simple fact that transports and freight activities physically bring the facilities of a supply chain together. Therefore, risks, uncertainties, and vulnerabilities in the supply chain and the transport network affect, contribute, and neutralize each other. Supply chain security is indented to safeguard the supply chain (in this meaning the transport and freight activities) from different antagonistic threats and thereby reduce the vulnerability of modern global trade.

Author details

Daniel Ekwall
School of Engineering, University of Borås, Borås, Sweden
Supply Chain Management and Corporate Geography, Hanken School of Economics, Helsinki, Finland

6. References

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

[2] Waters, D. (2007),"Supply chain risk management: vulnerability and resilience in logistics". Kogan-page, London

[3] Ekwall, D. (2009) *Managing the Risk for Antagonistic Threats against the Transport network*, Division of Logistics and Transportation, Chalmers University of Technology: Göteborg.

[4] Christopher, M (2005), *Logistics and Supply Chain Management – Creating Value-adding Networks*, Prentice Hall, London

[5] Bowersox, D.J. and Closs, D. J. and Cooper, M. B. (2002), *Supply Chain Logistics Management*, McGraw Hill/Irwin series, Boston (2nd Edition)

[6] Lumsden, K. (2006), *Logistikens grunder*. Studentlitteratur, Lund (*in Swedish*)

[7] Ruijgrok, C. and Wandel, S., and Nemoto, T. (1991). "Advanced Logistics and Road Freight Transport", *OECD Road Transport Research*, Chapter IV

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

[9] Ekwall, D. (2010), "On analyzing the official statistics for antagonistic threats against transports in EU: a supply chain risk perspective". *Journal of Transportation Security*, Vol. 3, No. 4, pp 213-230

[10] Francis, T. L. (1986), "A dynamic model of corruption deterrence. *Journal of Public Economics*, Vol. 31, pp 215-236

[11] Eurostat, 2009, *Criminal and criminal justice*. Statistics in focus 36/2009

[12] EUICS (2005), *The Burden of Crime in the EU, A Comparative Analysis of the European Survey of Crime and Safety*. (EU ICS).

[13] NRSS (2002), *National Retail Security Survey*. University of Florida

[14] ECR (2003), *Shrinkage: A Collaborative Approach to Reducing Stock Loss in the Supply Chain*. ECR Europe, Brussels, Belgium

[15] TAPA (2006), TAPA Loss Data Benchmark Survey 2006.

[16] Anderson, B. (2007), "Securing the Supply Chain – Prevent Cargo Theft". *Security*, No 5, Vol. 44, pp. 56-58

[17] EP - European Parliament's Committee on Transport and Tourism, (2007), *Organised theft of commercial vehicles and their loads in the European union*. European Parliament, Brussels

[18] ECMT (2001), *Theft of goods and goods vehicles*. CEMT/CM (2001)19, Lissabon.

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

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

[21] Barth, S. and White, M. D. (1998), "Hazardous cargo". World Trade, November 1998, pp. 29,
[22] Tryon, G. and Kleiner, B. (1997), "How to investigate alleged employee theft properly". *Managerial auditing journal*, Vol. 12, MCB University Press.
[23] Robinson P. V. (2009), "Freight crime in Europe: what happens next?". *A presentation at ESCB 09*, Prague
[24] Muir, J. (1996), "Theft at work". *Work Study*; Vol. 45.
[25] Beck, A. (2002), "Automatic product identification & shrinkage: Scoping the potential". *ECR Europe*, Brussels, Belgium
[26] Europol, (2009), *Cargo theft report: Applying the Brakes to Road Cargo Crime in Europe*. Europol, The Hague
[27] Napoleoni, L (2004), *Terror inc*. Penguin books ltd.
[28] Europol (2010), "EU Terrorism Situation and Trend Report 2010". The Hague, Netherlands
[29] Johnston, R. B. and Nedelescu, O. M. (2006), "The impact of terrorism on financial markets". *Journal of Financial Crime*, Vol. 13, No. 1, pp. 7-25
[30] Rystad, G. (2006), *Politiska mord – det yttersta argumentet*. Historiska media, Lund (in Swedish)
[31] Sjöberg, L. (2008), "Antagonism, trust and perceived risk". *Risk Management*, 10**,** 32 – 55. doi: 10.1057/palgrave.rm.8250039
[32] Gearson, J. (2002), "The nature of modern terrorism". *The political quarterly publishing*, pp. 7-24
[33] Burke, R. J. (2005), "International terrorism and threats to security: Implications for organizations and management". *Disaster Prevention and Management*, Vol. 14, No. 5, pp. 639-643
[34] Aggarwal, R. and Bohinc, J. (2011), "Black swans and supply chain strategic necessity". *Journal of Transportation Security*, DOI 10.1007/s12198-011-0080-5
[35] Rodwell, S. and Van Eeckhout, P. and Reid, A. and Walendowski, J. (2007), *Study: Effects of counterfeiting on EU SMEs and a review of various public and private IPR enforcement initiatives and resources*. Framework contract B3/ENTR/04/093-FC-Lot 6 Specific agreement n°SI2.448309
[36] EU Commission (2008), *Public Consultation in preparation of a Legal Proposal to combat counterfeit medicines for Human Use - Key Ideas for better Protection of Patients against the risk of Counterfeit Medicines*, Brussels
[37] DEA, U.S. Drug Enforcement Administration, (www.dea.gov)
[38] Bouchard, M. (2007), "On the resilience of illegal drug markets". *Global crime*, Vol. 8, No. 4, pp. 325- 344
[39] 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.
[40] EC, European Commission: Combating counterfeit & piracy, The economic consequences, (ec.europa.eu)

[41] Ekwall, D. (2009), "The risk for detection affects the logistics system setup for cargo smugglers". *In proceedings of Nofoma 2009*, Jönköping.
[42] Naylor, R (2004), *Wages of crime.* Cornell University Press. Ithaca.
[43] Antonopoulos, G. A. (2007), "Cigarette smugglers: A note on four "unusual suspects"". *Global crime*, Vol. 8, No. 4, pp. 393-398
[44] Jannati, F. and Salimi, M. (2011) *Modern Sea piracy - Modus operandi and economical and development state backgrounds*. School of Engineering, University of Borås, Sweden
[45] Abeyratne R (2010) Managing the twenty-first century piracy threat. In: Thomas A (ed) Supply chain security, Vol. 1. ABC-CLIO, Santa Barbara
[46] Sullivan, A. (2010), "Piracy in the Horn of Africa and its effects on the global supply chain". *Journal of Transportation Security*, Vol. 3, No. 4, pp. 231-243
[47] Onuoha. F, C, (2009), "Sea piracy and maritime security in the Horn of Africa: The Somali coast and Gulf of Aden in perspective". African Security Studies, Vol. 18, No. 3, pp. 31-44
[48] Madden, M. (2009), "Trading the Shield of Sovereignty for the Scales of Justice: A Proposal for Reform of International Sea Piracy Laws". *University of San Francisco Maritime Law Journal,* Vol. 21, No. 2, pp. 139-166.
[49] IMO (2011) *Ship and Shipping Facts & Figures – Information Resources on Trade, Safety, Security, and Environment*. Maritime Knowledge Centre, IMO
[50] 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.
[51] Solem, O. (2003), "Epistemology and logistics: A critical overview". *Systemic practice and action research*, vol 16, no. 6, pp. 437-454
[52] Arlbjörn, J.S. and Halldorsson, A. (2002), "Logistics knowledge creation: reflections on content, context and processes". *International journal of physical distribution & logistics management*, Vol. 32, No. 1, pp. 22-40.
[53] Gubi, E., and Arlbjørn, J.S., and Johansen, J. (2003), "Doctoral dissertations in logistics and supply chain management. A review of Scandinavian contributions from 1990 to 2001". *International Journal of Physical Distribution & Logistics Management*, Vol. 33, No. 10, pp. 854-885.
[54] Aastrup, J. and Halldórsson, A (2008), "Epistelmological role of case studies in logistics: a critical realist perspective". *International journal of physical distribution & logistics management*, Vol. 38, No. 10, pp. 746-763.
[55] Sarnecki, J. (2003), *Introduktion till kriminologi*. Studentlitteratur, Lund (*in Swedish*)
[56] Sherman, L.W. and Gartin, P. R. and Buerger, M. E. (1989), "Hot spots of predatory crime: routine activities and the criminology of place. *Criminology*, Vol. 27, No. 1, pp. 27-55
[57] Sampson, R. and Eck, J.E. and Dunham, J. (2010), "Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure". *Security Journal,* Vol. 23, No 1, pp. 37–51.

[58] Mankiw, N.G. (1997), *Principles of microeconomics*. The Dryden Press, Fort Worth Texas.

[59] Bodman, P. and Maultby, C. (1997), "Crime, punishment and deterrence in Australia". *International journal of social economics*, Vol 24. pp 884-901.

[60] Gigerenzer, G. and Reinhard, S. (2002), *Bounded Rationality: The Adaptive Toolbox*. Cambridge, MA: MIT Press.

[61] Simon, Herbert A. 1982. Models of Bounded Rationality. Cambridge, MA: MIT Press.

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

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

[64] Kroneberg, C. and Heintze, I. and Mehlkop, G. (2010), "The interplay of moral norms and instrumental incentives in crime causation". *Criminology*, Vol. 48, No. 1, pp 259-294

[65] Bergman, M. (2007), Straff och nåd speglar samhället. *Svenska Dagbladet*, november 2 (*in Swedish*)

[66] 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.

[67] Badolato, E.V. (2000), "Smart moves against cargo theft". *Security Management*, No 7, Vol. 44, pp. 110-115

[68] Tarnef, B. (2006), "Combating Cargo Theft". *American Agent & Broker*, Vol. 78, No. 10.

[69] Williams, R. and Bertsch, B. and Dale, B. and van der Wiele, T and van Iwaarden, J and Smith, M. and Visser, R. (2006), "Quality and risk management: what are the key issues?". *The TQM Magazine*, Vol. 18, No. 1, pp. 67-86

[70] Felson, M. (1987), "Routine activities and crime prevention in developing metropolis". *Criminology*, Vol. 25, No. 4, pp. 911-932

[71] Ekwall, D. (2009), "The Displacement effect in cargo theft". *International Journal of Physical Distribution and Logistics Management*, Vol. 39, No. 1, pp. 47-62

[72] Purtell, D. and Rice, J. B. (2006), "Assessing cargo supply risk". *Security management*, November, pp.78-87, ASIS international.

[73] Urciuoli, L. (2008), *Security in Physical Distributions*. Department of Industrial Management and Logistics, Lund University: Lund

[74] Speed, M. (2003), "Reducing employee dishonesty: In search of the right strategy". *Security journal*, Vol. 16, No. 2, pp 31-48, Perpetuity Press.

[75] 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.

[76] Lab S. P. (2000), *Crime prevention: Approaches, practices and evaluations*. Fourth edition. Andersson Publishing Co, Cincinnati US.

[77] Clarke, R. V. (1992), *Situational crime prevention: Successful case studies*. Harrow and Heston, New York.

[78] 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.
[79] Tyska, L.A. and Fennelly, L.J. (1983), *Controlling cargo theft*. Woburn: Butterworth Publishers, Boston.
[80] Crawford, A. (1998), *Crime prevention and community safety: Politics, policies and practice*. Longman London.
[81] Borodzicz, E. P. (2005), *Risk, crisis & security management*. Wiley, Chichester
[82] Reppetto. T. A. (1976), "Crime prevention and the displacement phenomenon". *Crime and Delinquency*, Vol. 22, pp. 166-177.
[83] Hesseling, R. (1994), "Displacement: A review of the empirical literature". In, Clarke, R. (ed.) *Crime prevention studies,* Vol 3, pp. 197-230. Monsey, NY: Criminal Justice Press.
[84] 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.
[85] 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.
[86] 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.
[87] Manunta, G. (2002), "Risk and security: Are they compatible concepts?". *Security journal*, Vol. 15, No. 2, pp 43-55, Perpetuity Press.
[88] Clutterbuck, R. (1987), *Kidnap, hijack and extortion*. Basingstoke Macmillan, London
[89] Ekwall, D. and Nilsson, F. (2008), "Using business complexity to handle supply chain risk: Dealing with borders of cargo liability". *In proceedings of Nofoma 2008*, Helsinki
[90] Ekwall, D. and Nilsson, F. (2011), "Reallocation of risks within supply chains: The practice of enhanced liability clauses". *In proceedings of Nofoma 2011*, Harstadt
[91] Kelly, M. and Kleffner, A. E. (2003), "Optimal Loss Mitigation and Contract Design". *The Journal of Risk and Insurance*, Vol. 70, No. 1, 53-72
[92] Mears-Young, B. and Jackson, M. (1997), **"**Integrated logistics - call in the revolutionaries". *Omega,* Vol. 25, No. 6, pp. 605-618.
[93] Gentry, J. (1996), "Carrier involvement in buyer-supplier strategic partnerships". *International Journal of Physical Distribution & Logistics Management*, Vol. 26, No 3, pp.14-25.
[94] Lambert D. and Cooper, M. and Pagh, J. (1998), "Supply Chain Management: Implementation Issues and Research Opportunities". *The International Journal of Logistics Management*, Vol 9, No 2, pp.1-20

[95] Yu, Z. and Yan, H. and Cheng, E. (2001), "Benefits of information sharing with supply chain partnerships". *Industrial Management & Data Systems*, Vol. 101, No. 3, pp. 114-121.

[96] Cox, A. and Ireland, P. and Lonsdale, C. and Sanderson, J. and Watson, G. (1992), *Supply chains, markets and power: mapping buyer and supplier power regimes*. Routledge, London

[97] Cox, A. (2001): The Power Perspective in Procurement and Supply Management. *Journal of Supply Chain Management*, Vol. 37, nr. 2, ss. 4-7

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

[99] Sweet, K. (2006), *Transportation and Cargo security*. Pearson Prentice Hall, New Jersey.

[100] Lee, H.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.

[101] Manuj, I. and Mentzer, J.T. (2008), "Global supply chain risk management strategies". *International Journal of Physical Distribution & Logistics Management*, Vol. 38, No. 3, pp. 192-223

[102] Ritter, L. and Barrett, J. M. and Wilson, R. (2007), *Securing global transportation networks*. McGraw Hill, NY

[103] Sarathy, R. (2006), "Security and the global supply chain". *Transportion journal*, fall, pp.29-51

[104] Sheu, C. and Lee, L. and Niehoff, B. (2006), "A voluntary logistics security program and international supply chain partnership". *Supply Chain Management: An International Journal*, Vol. 11, No 4, pp.363–374.

[105] Fletcher, T. (2007), "Authorised economic operator (AEO) programs: IBM's perspective". *World Customs Journal*, Vol. 1, No. 2, pp 61-66

[106] Gutiérrez, X. and Hintsa, J. and Wieser, P. and Hameri, A-P. (2007), "Voluntary supply chain security program impact: an empirical study with basc member companies". *World Customs Journal*, Vol. 1, No. 2, pp 31-48

[107] Grainger, A. (2007), "Supply chain security: adding to a complex operational and institutional environment". *World Customs Journal*, Vol. 1, No. 2, pp 17-30

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

[109] Mazeradi, A. and Ekwall, D. (2009)," Impacts of the ISPS code on port activities – A case study on Swedish ports". *World Review of Intermodal Transportation Research, Vol. 2, No. 4*, pp. 326-342

[110] Powanga, L. (2006), "A business perspective of US International Seaborne Security Measures: Impact on Importers". *Journal of Global Business*, Vol. 33, pp.63-75

[111] Haughton, M.A. (2007), "Examining the business case for shipper participation in Canada USA trade security programmes". *International Journal of Logistics Research and Applications*, Vol. 10, No. 4, pp.315-331

[112] Willys, H.H. and Ortiz, D.S. (2004). "Evaluating the Security of the Global Containerized Supply Chain," RAND Corporation, Santa Monica, CA.

[113] www.tapaemea.com

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