DEFENCE SUPPLY CHAIN MANAGEMENT: CONCEPTUAL FRAMEWORK AND FIRST EMPIRICAL FINDINGS

Michael Essig, Sandra Tandler and Michael Scheckenhofer

Michael Essig, Chair of Materials Management and Distribution, Director of the Research Center for Law and Management of Public Procurement (FoRMöB)

Sandra Tandler, Scientific assistant at the Research Center for Law and Management of Public Procurement (FoRMöB)

Michael Scheckenhofer, Scientific assistant at the Research Center for Law and Management of Public Procurement (FoRMöB)

ABSTRACT

National defence in today's complex, globalized and asymmetric security situation is facing numerous challenges which demand for a more comprehensive designed foreign and security policy in the sense of a new management approach. This does not only imply a closer collaboration between all relevant organisations, be they governmental or not. Rather, safety- and security-related instruments have to be implemented as well in order to further ensure national defence. Thus the article aims to achieve two main goals: Firstly, in using private sector research results on supply chain management, the defence sector and its members, associated links, structures and processes are analyzed (theoretical deductive). Secondly, the relevance, and method of implementing safety- and security-related instruments will be – while taking a case study conducted in German defence supply chains into account – emphasized (empirical inductive). With the combination of both approaches efficiency and effectiveness in the defence sector can be positively influenced.

INTRODUCTION

As the security policy situation is currently characterised by threats from international terrorism, proliferation of weapons of mass destruction, and regional and ethnic conflicts (Hartley, 2006), states are being encouraged to produce and maintain national security (Hartley, 2002a). According to the constitution (in Germany: Article 87 a GG), the resulting spectrum of tasks is incumbent upon the armed forces, which can be regarded as an instrument within the purview of the defence portfolio. As the armed forces are part of the public sector, they have to be provided with financial resources by the government. In this context, the Stockholm International Peace Research Institute (SIPRI) (2009) estimated that worldwide military expenditures amounted to US $1.464 trillion in 2008 (cf. SIPRI, 2009). The USA alone, being the most influential nation, accounts for a 41.5% share of the total sum (i.e., 607 billion in US dollars). In view of these huge sums being spent on the maintenance of national security, armed forces have, for several years now, been faced with an increased pressure to reduce costs (Tatham, 2005; Hartley, 2002a).

Due to its focus on improving military procurement, the so-called Defence Package recently adopted by the European Commission can be seen as a potential tool to meet these challenges. The relevance of the Defence Package derives from the fact that national markets have been walled off for more than 40 years with regard to defence material, which has been concomitant with an impairment of the production and procurement of high-quality armament products at affordable cost (cf. Commission of the European Communities, 2007). Based on this, the Commission of the European Communities has adopted two directives which have to be transposed by EU member states into their national legislation within the next two years: Directive 2009/81/EC on defence and security procurement, and directive 2009/43/EC on intra-EU transfers of defence products, simplifying terms and conditions of transfers of defence-related products within the Community (European Commission, 2009). These directives specify the conditions for making use of Article 296 EC Treaty (exclusionary rule acknowledging the right of EU member states to exempt defence procurement contracts from Community rules), aiming to improve adherence to the treaty and to open the defence markets (Commission of the European Communities, 2007).

Despite this, to meet the armed forces' challenges, another potential tool can be seen in the concept of Supply Chain Management (SCM). As they are confronted with the pressure to ensure efficiency while, at the same time, taking into consideration the pressure to ensure operational effectiveness, armed forces need to concentrate on their core competencies and to make use of modern forms of cooperation and financing. This trend is expressed by the realization of various Public Finance Initiatives (PFI) or Public Private Partnerships (PPP), which has been intensified within the last years (Hartley, 2002b). Against that background, issues referring to the adoption of business concepts that have been originally developed both in and for the private sector are increasingly brought to the centre of the public sector's debate. Due to its contribution to the realization of cost-, time-, and quality-related advantages (Ellram/Birou, 1995), SCM can be considered to represent an adequate tool to overcome the armed forces' challenges. However, taking into consideration their specifics (Boyne, 2002; Rogers, 1981), an undifferentiated transfer of private sector's management practices to the public sector – or to the armed forces – cannot be recommended. Rather, what must be developed is an armed forces-specific concept in the sense of a Defence SCM.

Thus, one main objective of this paper is to develop a conceptual framework of a specific management concept for armed forces. In order to accomplish this, defence supply chain structures and processes will be analysed. Along with this, the relevance of a safety- and security-related management component will be derived, followed by the introduction and discussion of Supply Chain Safety Management (SCSM). Based on this, another main objective of this paper is to examine empirically whether SCSM, within the framework of Defence SCM, can be considered to be an adequate management component. Given these intentions, the paper is divided into two sections: Section one will include the conceptual development of Defence SCM – the procedure carried out here will be theoretically deductive. Section two will include the empirical examination of SCSM by means of a pilot case study

– the procedure carried out here will be empirically inductive. The paper will conclude by giving an outlook on the further need for research.

CONCEPTUAL FRAMEWORK OF DEFENCE SCM

Basics of SCM

Since the early 1980s, SCM has been intensively discussed and practiced in science and in industry. The term "Supply Chain Management" was introduced in 1982 by Oliver/Webber (Oliver/Webber, 1982). Despite its popularity, a common understanding of SCM has not yet evolved (Mentzer et al., 2001). The lack of a generally accepted definition of SCM is ascribed to the fact that the SCM concept was not elaborated in business administration science. In fact, the SCM concept has its origins in business practice (i.a., Lambert/Cooper, 2000; Cooper/Lambert/Pagh, 1997). Thus, the (scientific) discussion relating to the term and concept of SCM is multifaceted, as is shown by the following examples:

- Simchi-Levi/Kaminsky/Simchi-Levi (2000) define SCM as "[…] set of approaches utilised to efficiently integrate suppliers, manufacturers, warehouses, and stores so that merchandise is produced and distributed at the right quantities, to the right locations, and at the right time in order to minimise system-wide costs while satisfying service level requirements."
- Christopher (1998) defines SCM as "[…] the management of upstream and downstream relationships with suppliers and customers to deliver superior customer value at less cost to the supply chain as a whole. […] Thus the focus of supply chain management is upon the management of relationships in order to achieve a more profitable outcome for all parties in the chain."
- Cooper/Lambert/Pagh (1997) define SCM as "[…] the integration of business from end-users through original suppliers that provide products, services and information that add value for customers […]."

Despite the absence of a generally accepted definition of SCM, no reference model prevails in literature or in practice. Rather, a number of SCM reference models coexist that can be used for the management of supply chains, e.g. the framework of Mentzer et al.

(2001), the Bowersox framework (1997), the model of Cooper/Lambert/Pagh (1997), the model of Metz (1997), the SCOR model of the Supply Chain Council (1996), and the model of Lambert/Emmelhainz/Gardner (1996). Due to its high prevalence and acceptability in scientific literature, the SCM framework developed by Cooper/Lambert/Pagh (1997) will be chosen for the development of Defence SCM. The SCM framework consists of three central conceptual elements deemed relevant to the comprehensive management of supply chains (cf. figure 1):

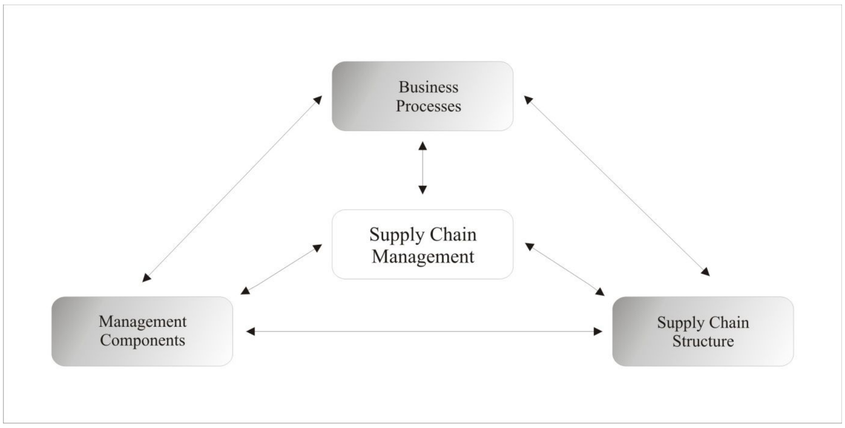

Figure 1: Elements of the SCM framework (source: Cooper/Lambert/Pagh, 1997).

(1) *Supply chain structure* includes the identification of the key supply chain members, among whom business processes are to be linked via SCM.

(2) *Business processes* deals with the question of *which processes* should be linked among the key supply chain members.

(3) *Management components* help to determine the degree of integration of processes and management for planning, operating and controlling the supply chain (Cooper/Lambert/Pagh, 1997).

Given the aim of conceptualising Defence SCM, the character of each element previously mentioned will be analysed now from the armed forces' perspective.

Defence supply chain structure

From the point of view of a nation, the following can generally be counted among the main actors of defence supply chains: its citizens, its political level of decision making, its armed forces, other nations' armed forces, its defence administration (responsible for procurement procedures), international agencies (e.g., for armaments collaboration), civilian (logistics) service providers, the armaments industry, suppliers of other goods that are necessary for the production of national security, and public private partnerships (cf. Dorobek/Eßig/Klein-Schmeink, 2009). Each of these network nodes is assigned to either the public or the defence or the private sector. The following figure illustrates the resulting defence supply chain structure in detail (cf. figure 2):

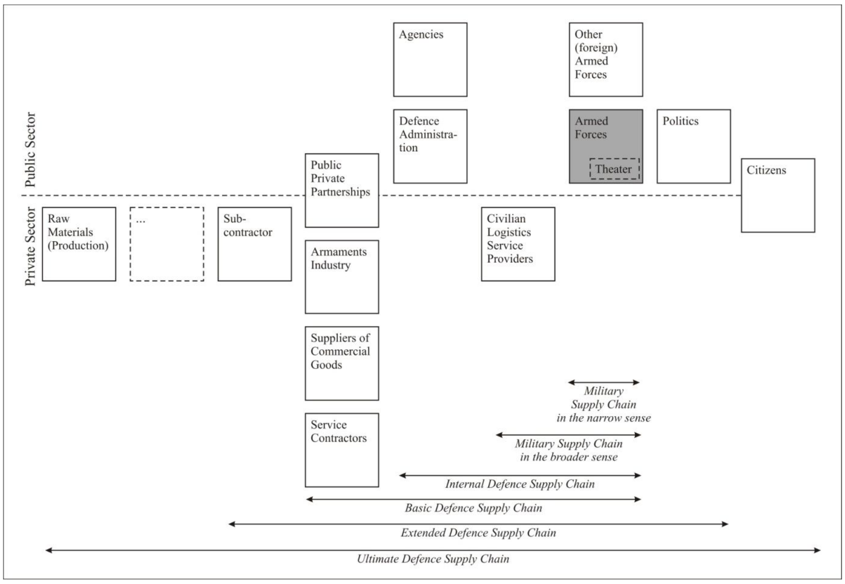

Figure 2: Defence supply chain structure (source: authors, based on Dorobek/Eßig/Klein-Schmeink, 2009).

The discussion about how to processually link the identified actors in the sense of Defence SCM leads to the deduction of various types of defence supply chains. The initial point of the defence supply chain, and therefore the “ordering party”, are the citizens, who are as a whole interested in a peaceful life. The political goal of safeguarding a peaceful and liberal cohabitation and thus the public task of ensuring national security are derived therefrom (Eichhorn, 2001). It is a decision on the political level to set up armed forces to fulfil this task (in Germany: Article 87 a GG). The armed forces themselves are the core element of military service delivery, and thus the focal institution. The key performance feature is military operations (abroad), which are usually carried out in cooperation with the armed forces of other nations. This scope of activity can be considered as the *Military Supply Chain in the narrow sense*, that is, the joint operation of military forces, for which only soldiers are deployed. By contrast, the term *Military Supply Chain in the broader sense* refers to a structure in which private logistics service providers are integrated who perform transportation services in the logistics network.

As a rule, the armed forces themselves are not responsible for the procurement management of the defence supply chain. Rather, this is the role of the defence administration, that is, the civilian branch of the armed forces (in Germany: Article 87 b GG). The defence administration acts as an interface to the private sector, meeting the demand of the armed forces through public invitations to tender for the provision of goods and services. This task can be transferred to so-called “agencies”, which take over the fulfilment of demand in international cooperation. Examples include the European OCCAR (Organisation Conjointe de Coopération en matière d'Armement) and the NATO Maintenance and Supply Agency (NAMSA), which is responsible for the NH90/TIGER helicopter program, among other projects. However, as the defence administration is involved, which is not only a civilian institution but also part of the military organisation, this may well be referred to as an *Internal Defence Supply Chain*.

According to Mentzer et al. (2001), the term *Basic Defence Supply Chain* is used when taking an integrated view of the immediate customers and the immediate suppliers of the focal institution (armed forces) (Mentzer et al., 2001). The immediate customer is the soldier in the field; immediate suppliers are either private companies or PPP, which are jointly operated by the armed forces and private partners. The group of private companies can again be subdivided into the armaments industry, suppliers of commercial goods, and civilian service contractors. By contrast, the term *Extended Defence Supply Chain* refers to a structure in which subcontractors and the political level as the direct "consumer" of security services are included. Finally, the *Ultimate Defence Supply Chain* comprises the entire defence-related supply chain, ranging from the citizen as the ultimate end customer to the defence policy sphere, to the armed forces and the defence administration and to all levels of suppliers and contractors back to the producers of raw materials.

The analysis of the element *structure* has shown that defence supply chains involve a large number of various actors which can be distinguished in terms of their corresponding geographic (national and international) and sectoral (private, public, and defence) levels. The associated fragmentation of the spectrum of operations fulfilled by the armed forces results in an increased interface complexity which, in the course of Defence SCM, reveals the necessity to integrate safety- and security-related aspects.

Defence supply chain processes

The change from function to process orientation can be considered the main prerequisite of successful SCM (Lambert/Cooper, 2000). The Global Supply Forum (1996) identified nine business processes that should be taken into account. These include Customer Relationship Management, Customer Service Management, Demand Management, Order Fulfilment, Manufacturing Flow Management, Procurement, Product Development and Commercialization, and Returns Channel (for a detailed description see Lambert/García-Dastugue/Croxton, 2005). As the business processes previously mentioned are predominantly addressed to private supply chains, the unreflected transfer to defence supply chains should be avoided. Instead, the focus is on logistics, as this process might be considered as the most relevant in the analysis of defence supply chains (Mathaisel/Manary/Comm, 2009). According to the North Atlantic Treaty Organization (NATO), the term is defined as the science of planning and carrying out the movement and maintenance of forces (NATO, 2007). In its most comprehensive sense the logistics process comprises all aspects of military operations that enable the armed forces to cope with their spectrum of tasks. Generally, this includes the following categories or subprocesses (cf. NATO, 2007): design and development; acquisition, storage, transport, distribution, maintenance, evacuation and disposal of materiel; transport of personnel; acquisition, construction, maintenance, operation and other uses of facilities; acquisition or furnishing of services; and medical and health service support.

However, these subprocesses recommended by NATO are applied in different ways by the respective armed forces. For example, the logistics process of the German armed forces is embedded in a process model which had been defined in the course of the planned SASPF ERP solution implementation that began in 2000. The process model consists of nine primary processes, which can be further subdivided into core processes (these include armaments/logistics, personnel and health care), control processes (these include Bundeswehr planning, accounting, organisation and controlling) and support processes (these include individual training, infrastructure and environmental protection) (BMVg, 2001). The process of armaments/logistics in turn is partitioned into several subprocesses (cf. BMVg, 2001):[1]

- *Logistics command* includes the totality of planning, regulating and controlling measures that are necessary to ensure the optimum interaction of all logistics forces and resources and, thus, to ensure the logistics support of the armed forces during peacetime and wartime.
- *Procurement and storage* includes the acquisition or leasing of products and the rendering of services.

---

1 The process model defined by the German armed forces is quite similar to that defined by the Swiss armed forces. Their process model is subdivided into management processes (these include logistics planning and logistics command), core processes (these include supply and return, maintenance, and medical services) and support processes (these include movement and transportation as well as infrastructure). See Hofstetter/Stölzle (2009).

- *Materials management* includes the time- and demand-oriented provision of material at the end customer as well as relieving the end customer of material that is not required anymore.
- *Technical logistics management* includes all tasks that refer to the creation and modification of material-related data.
- *Maintenance and manufacturing* includes the assessment, maintenance, conservation, repair and manufacturing of materials.
- *Exploitation* includes the further disposal of material and waste in the broadest sense that are no longer in use.
- *Movement and transportation* includes the planning, coordination, control and monitoring of all activities which serve to mobilise personnel and/or material for military purposes at home and abroad, as well as military automotive affairs.
- *Material delivery* includes the delivery of physical parts and is closely connected with the *procurement and storage* subprocess.

Based on the subprocesses discussed above, it becomes clear that the definition of the logistics process made by the German armed forces is closely related to the definition of logistics processes recommended by NATO. Apart from that, parallels can be drawn between the processes recommended for defence supply chains and those recommended for private supply chains within the SCM framework of Cooper/Lambert/Pagh (1997): The processes *procurement and storage* (cf. SCM framework of Cooper/Lambert/Pagh (1997): procurement), *exploitation* (returns channel) and *material delivery* (order fulfilment) should be mentioned here as examples.

Nevertheless, one central aspect has to be taken into account in the analysis of the processes of defence supply chains: The armed forces need to distinguish between two types of scenario (Tatham, 2005) which play a decisive role in determining the scope of the processes and the strategy to be chosen (cf. figure 3):

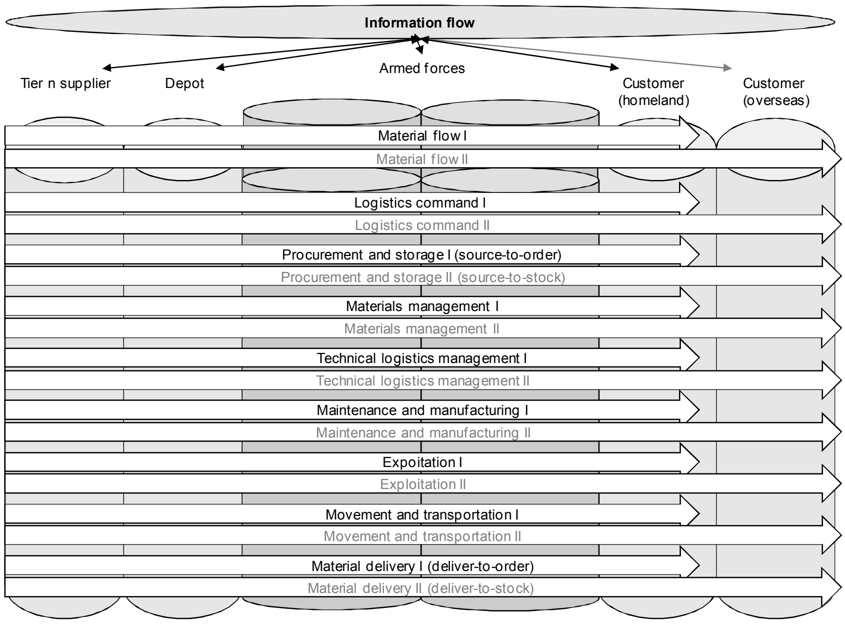

Figure 3: Defence supply chain business processes (source: authors).

Scenario I reflects the state of peacetime – the spectrum of tasks fulfilled by armed forces is then performed at home only. As a result, the processes of defence supply chains are characterised in that the scope of consideration is limited to the national territory. In this context, the German armed forces refer to the term *basic logistics* (BMVg, 2004). By contrast, Scenario II reflects the state of wartime – the spectrum of tasks fulfilled by armed forces is then performed in an area of operation. In consequence, the processes of defence supply chains are characterised by a scope of consideration that also includes the respective area of operation. For this, the German armed forces use the term *logistics support operations* (BMVg, 2004).

By considering the two scenarios, conclusions can be drawn as to the scope of defence supply chain processes. This finding, however, leads to the question of which type of strategy should be chosen. Basically, the level of risk that the military end customer is facing as well as the target structure of defence supply chains can be considered as the initial points: During peacetime the military end customer is located in Germany – thus, the disruption of the continuity of supply does not have life-threatening consequences. For this purpose, defence supply chains should be geared towards efficiency-based considerations, and, therefore, on the minimisation of costs. The adoption of a lean supply chain strategy is then recommended (Tatham, 2005). In wartime, however, the need to ensure the continuity of supply is of vital importance, as a disruption may have life-threatening consequences for the military end customer stationed in the area of operation. Consequently, the peacetime goal of cost minimisation of defence supply chains is no longer suitable during actual operations. Rather, there is a need to take effectiveness-based considerations into account and, thus, to adopt an agile supply chain strategy (Tatham, 2005).

As they need to maintain their capability of conducting military operations at all times, armed forces are facing a key dilemma, (Tatham, 2005; Lai, 2003): They are subject to the challenge of overcoming the relation between conflicting goals, that is, the adoption of a lean supply chain strategy to focus on the minimisation of costs (during peacetime) on the one hand, and the adoption of an agile supply chain strategy to focus on building up capacities and capabilities (during wartime) on the other hand (Tatham, 2005). Therefore, given the need to take into consideration both cost-related and safety-, respectively security-related objectives, the question as to which strategy is to be considered adequate for defence supply chains requires a critical and more detailed verification.

Excursus: Defence supply chain strategies

The assumption that there is a single strategy equally suitable to all types of supply chains has been – in accordance with the "one size does not fit all"-principle (Shewchuk, 1998) – regarded as obsolete, at least since the article "What Is the Right Supply Chain for Your Product?" was published in 1997 by Fisher. Rather, the right strategy should be determined by taking several criteria into account. In this context, Fisher (cf. Fisher, 1997) postulates that the choice of the right supply chain strategy depends on the characteristics of the product. Therefore, he distinguishes between functional and innovative products showing different degrees of certain criteria such as type of demand, product life cycle, or product variety. Functional products require the adoption of physically efficient (i.e., lean) supply chains, while innovative products require the adoption of market-responsive (i.e., agile) supply chains. According to Naylor/Naim/Berry (1999), the types of strategies differ in that "[...] Leanness means developing a value stream to eliminate all waste including time, and to enable a level schedule [...]", whereas "[...] Agility means using market knowledge and a virtual corporation to exploit profitable opportunities in a volatile marketplace [...]" (Naylor/Naim/Berry, 1999).

In scientific literature, a number of authors can be identified who have further developed and modified Fisher's approach to systematisation.[2] In this regard, one major finding can be seen in the renouncement of the strict (dichotomous) distinction between lean and agile strategies. This is based on the realisation that both strategies are, in principle, not mutually exclusive (Naylor/Naim/Berry, 1999). In addition to that, several examples – including defence supply chains– have revealed the need for the development of hybrid strategies (Christopher/Towill, 2000). Thus, approaches resulting from these considerations are characterised by an intensive debate referring to the systematisation of lean, agile, and leagile supply chain strategies. Christopher/Peck/Towill (2006), for instance, refer to the criteria *products* (standard – special), *demand* (stable – volatile), and *replenishment lead times* (short – long). The adoption of a leagile strategy is recommended in supply chains where the underlying products are characterised by their high levels of customisation, distribution in low quantities, long replenishment lead times and an unpredictable demand (Christopher/Peck/Towill, 2006). Based on this, parallels can be drawn that relate to the characteristics of defence supply chains. Thus, with approximately 5.2 million supply items

2 For a detailed overview on various approaches see Neher (2005). See Neher, 2005. As the overview given by Neher (2005) only refers to approaches published until 2003, some further authors (Christopher/Peck/Towill (2006), Jüttner/Godsell/Christopher (2006) and Vonderembse et al. (2006)) should be considered here as well.

(Mathaisel/Manary/Comm, 2009) passed through in defence supply chains, there is a high range of products varying from low complex (e.g., clothing) to high complex (e.g., nuclear weapons) products (Lai, 2003). As a consequence, the associated structure of demand tends to be poor (Mathaisel/Manary/Comm, 2009). Moreover, defence supply chains are characterised by long replenishment lead times (Lai, 2003). One possible reason for this is the high complexity of the procurement process, as it is mandatory for public institutions to adhere to the directives governing the procurement of goods and services. Another reason is to be seen in the long development times of military products in the course of defence acquisition.

Defence supply chain management components

The analysis of structures, processes, and strategies has revealed that defence supply chains are subject to particular challenges which require the adoption of appropriate management components. Firstly, both efficiency-based (i.e., cost minimisation) and effectiveness-based objectives (i.e., ensuring national security, the continuity of supply of the citizens, and of the military end customer, respectively) have to be taken into account (Dorobek/Eßig/Klein-Schmeink, 2009). Secondly – due to the fact that the armed forces constitute infrastructures that are of crucial relevance for the community and the failure or impairment of which have the potential to cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences –, safety and security-related measures are to be integrated to mitigate and to cope with damages (Federal Ministry of the Interior, 2005). Against this background, the approach called Supply Chain Safety Management (SCSM) whose primary objective is to achieve continuity of supply (i.e., effectiveness), while also taking the economic goal of profitability into consideration (i.e., efficiency) (Large, 2006; Steven/Tengler, 2005), will be introduced.

Due to the fact that the English language offers two specifications (safety vs. security), these terms have to be defined first from a supply chain perspective (Lange, 2005; Egger, 1992). Security can be interpreted as the protection of the material and immaterial elements of a supply chain against intended attacks in the form of organised crime and international terrorism (Lange, 2005; Matschke/Ick, 1998). In contrast to that, safety is being interpreted as a kind of protection from inherent hazards. This puts the focus on the protection against random events such as natural catastrophes or carelessness and negligence (Lange, 2005; Matschke/Ick, 1998). According to the authors, safety will be used as the comprehensive term and therefore should be understood to include measures taken to achieve security.

Considering the primary goal of ensuring the continuity of supply, all safety-related action alternatives should be aligned with the minimisation of disruptions that supply chains are faced with (Craighead et al., 2007). This means that the action alternatives of supply chain protection and supply chain resilience are combined into an all-encompassing integrated safety approach. Supply chain protection includes preventive action alternatives (e.g., data back-up, introduction of (international) standards and certifications), which are intended to avoid disruptions or interruptions of the supply chain (Sheffi et al., 2004; Lee/Wolfe, 2003; Deutch, 2002). Supply chain resilience includes reactive action alternatives (e.g., investments in infrastructure and resources, standardised facilities and processes, and postponement) that aim at allowing a supply chain to swiftly react to unexpected events (Rice et al., 2003). In the general framework of supply chain preparedness it is the stated goal to create a supply chain which reduces the likelihood of a possible interruption of supply and develops approaches to proactively react to a disruption in case that it should actually occur (Billington, 2002). The results up to now can be summarised in the following figure 4:

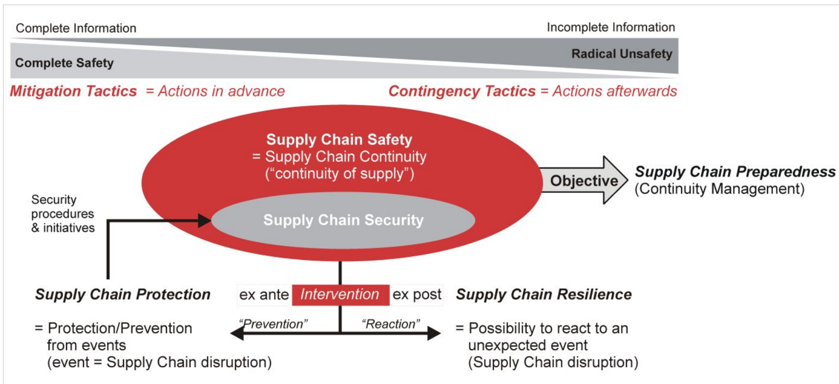

Figure 4: Supply chain safety management approach.

METHODS

Case study design

Based on the theoretical foundations discussed in the previous section, an empirical investigation is required now which aims to verify the suitability of the SCSM approach as an appropriate management component within defence supply chains. Therefore, the underlying research question is as follows:

How should the SCSM approach be implemented or integrated, respectively, in defence supply chains so that it contributes to the achievement of effectiveness-based objectives (ensuring national security, respectively the continuity of supply), while also taking efficiency-based objectives (cost minimization) into consideration?

Due to the explorative character and the nature of the research question ("how"), the case study method seems to be appropriate to meet the objective of the empirical investigation (Ellram, 1996). According to Eisenhardt (1989), random sampling is neither necessary nor even preferable (Eisenhardt, 1989). Based on this, the unit of analysis is chosen by means of purposive sampling (Patton, 1990). This procedure ensures that those cases will be taken into consideration which reflect the analysed phenomenon. In consequence (as explicitly stated within the research question), defence supply chains are considered to be the unit of analysis. In accordance with Marshall/Rossman (1995), the ideal unit of analysis is characterised by a rich mixture of processes, humans, and/or structures as well as by providing easy access for the researcher (Marshall/Rossman, 1995). These criteria are fulfilled: Firstly, access to the unit of analysis is ensured by a research project called Supply Chain Safety Management, as this multi-year project involves – besides a research team of the University of the Bundeswehr Munich – various actors of defence supply chains (including Armed Forces Staff S IV of the Federal Ministry of Defence, the Federal Office of Defence Technology and Procurement (BWB), the Bundeswehr Logistics Centre, and the Joint Support Command). Moreover, the type of the case study reflects the required rich mixture of processes, humans, and/or structures. This is based on the fact that defence supply chains can be perceived as an overall system in which various subsystems (including the procurement organisation (BWB), logistics service providers, depots, the Joint Support Command, the Joint Forces Command, or the Bundeswehr Logistics Centre) will be analysed. Consequently, an embedded single case study is used in the course of the empirical investigation (Yin, 2009). The following figure 5 highlights the overall system divided into its respective flows of information and material as well as its underlying subsystems:

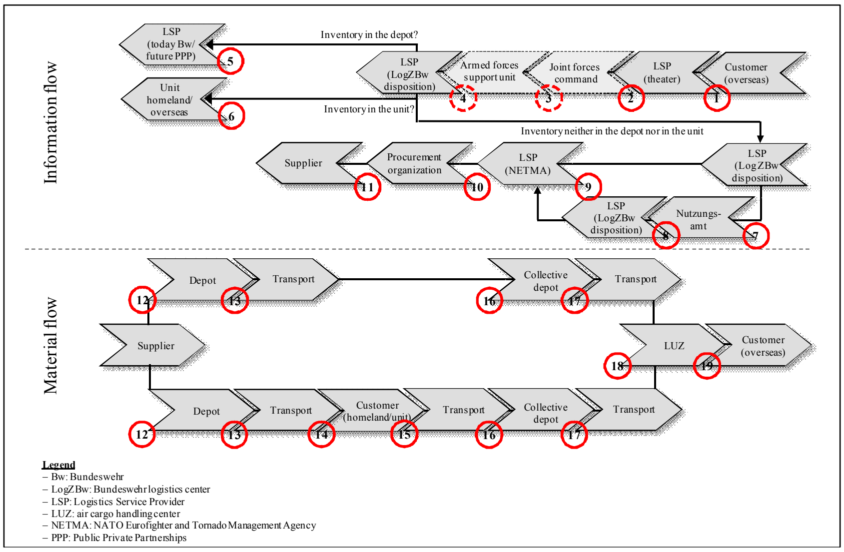

Figure 5: Overall system of the analysed defence supply chain and its sub-systems.

Preparation

The implementation or integration, respectively, of the SCSM approach within the analysed defence supply chain is based on the basic model of strategic planning (cf. Steiner, 1969), which is subdivided into the phases of goal formulation, strategic analysis, strategy formulation and implementation, and strategy control. Following the SCSM approach discussed above, ensuring continuity of supply is the underlying goal formulation. Due to the comprehensive character of the subsequent phases of the strategic planning process, the focus here is on the phase of strategic analysis, comprising the analysis of external and internal conditions. Consequently, risk factors which might adversely impair the continuity of supply of defence supply chains will be analysed in detail in the course of this paper. Therefore, a catalogue of instruments has to be developed which applies to all subsystems identified within the defence supply chain. Thanks to its generic character, the Failure Mode and Effects Analysis (FMEA) can be considered to be such an instrument, providing the basic grid to analyse, assess, and optimise risk factors that relate to the safety, and to the security of supply chains respectively.

Filling the first column (risk analysis) of the FMEA requires the selection of a further instrument which permits the fullest possible identification and systematisation of risk factors in supply chains. In this context, the approach of Christopher/Peck (2004) is chosen, as they have categorised supply chain risks into five categories (cf. Christopher/Peck, 2004): Process and control risks (internal to the firm), supply and demand risks (external to the firm but internal to the supply network), and environmental risks (external to the network). Items are subsequently formulated based on a literature review, which reflect factors that take into consideration both safety-and security-related aspects. Afterwards, joint project meetings were used to discuss the generic risk categories and their corresponding items with respect to their terminology and to their potential to disrupt the continuity of supply of the analysed defence supply chain. The remaining risk categories and items then have been translated into concrete statements. The enquiry of the statements *Opportunistic behaviour by third parties is feared*, or *The handling of business processes is influenced by terrorist or criminal acts*, for instance, help to gain a better understanding of the security of the analysed defence supply chain. By contrast, statements such as *Goods are not delivered to the right place*, or *Due to media breaks, data entered/transmitted are incomplete or contain an error* provide information about the safety of the analysed defence supply chain.

As to filling the second column (risk assessment), the FMEA offers a technique called risk priority number (RPN), which permits the assessment of each item based on three specific determinants: occurrence (O), detection (D), and severity (S). Prior to the actual assessment of risk factors, the identification and analysis of scaling methods that focus on measuring attitudes is required (Hogg/Vaughan, 2008). Again, joint project meetings have been used to choose the optimum scaling method – the Likert scale. Considering this, each item can be further refined on a five-point Likert scale (very high – high – medium – low – very low) with respect to the determinants O, D, and S. In detail, the calculation of the determinants O, D, and E each depends on the consideration of two criteria (cf. Table 1):

Table 1:

Determinant	**Criteria**
Occurrence	▪ How often does the item occur? ▪ Are there any possibilities (in terms of action measures) existing so far which might help to prevent the item from occurring?
Detection	▪ Is it assumed that, in reality, the item does occur even more frequently? ▪ Are there any possibilities (in terms of action measures) existing so far which might help to detect the item?
Severity	▪ Is there a realistic possibility to cope with the damage being caused by the item? ▪ What is the effort (in terms of financial, material, time, and personnel resources) required to cope with the damage?

Apart from this, as the Likert scale is lacking the possibility to simply ask for the existence of an item (“Yes”, “No”, “No knowledge”), a nominal scale will be used in supplement.

The procedure carried out here can also be described by means of a structural equation modelling known from empirical marketing research (cf. Byrne, 2009). Basically, structural equation modelling consists of a structural and a measurement model. The structural model helps to specify interdependencies that exist between latent exogeneous and latent endogeneous variables. Latent exogeneous variables exclusively explain other (latent) variables. However, latent endogeneous variables can, in addition, also be explained by other latent variables. The determination of these variables as well as their underlying interdependencies has to be carried out by the researcher on the basis of theoretical considerations. The measurement model, in turn, focuses on reflecting the relationship between each (exogeneous as well as endogeneous) variable and its corresponding indicators.

Building on this, the structural equation modelling of the underlying empirical investigation can be illustrated as follows:

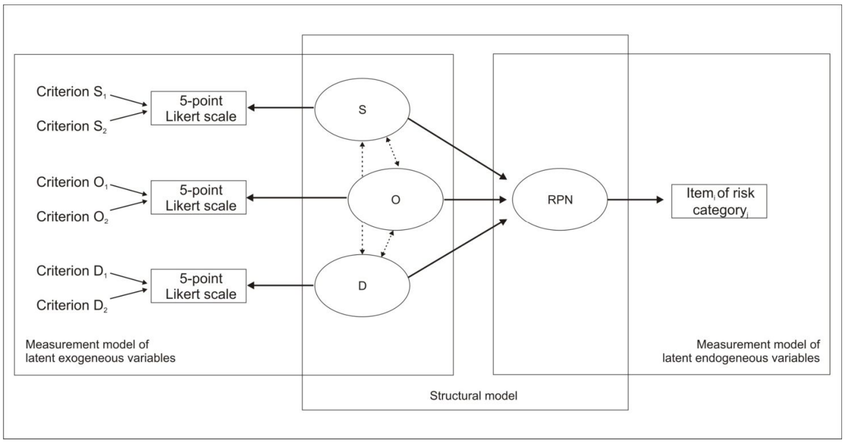

Figure 6: Structural equation modelling of the empirical investigation.

As highlighted in the figure, the RPN can be considered the latent endogeneous variable explaining the degree of risk of an item of a risk category. The RPN, in turn, is explained by its underlying determinants O, D, and S, which reflect the latent exogeneous variables of the structural model. The calculation of RPN is performed by multiplying O, D, and S, which are all equally weighted. Nevertheless, these three latent exogeneous variables themselves are interrelated with each other. In particular, the underlying interdependency becomes obvious if the value of RPN is identical for several items. RPN = 100, for instance, may result from both the calculation of O*S*D = 5*5*4 as well as O*S*D = 1*10*10, and, thus, has various reasons (Lewis/Dudley, 2005). Therefore, it is recommended not only to focus on the value of RPN as a whole but also to take a differentiated view with respect to the underlying determinants in terms of a top-down approach (Bertsche, 2008). Despite this, the measurement model for each of the three latent exogeneous variables is reflected by a five-point Likert scale and its corresponding criteria, which have been defined in table 1 (see table 1).

The phase of preparation is concluded by the construction of a questionnaire. In total, it comprises 55 items distributed to five risk categories and which are to be measured with regard to their occurrence and character in each subsystem of the analysed defence supply chain.

Data collection

In the course of explorative case studies, it is recommended to conduct a pilot case study in advance (cf. Yin, 2009). The latter can be referred to as a kind of feasibility study and aims to prevent the transferral of unverified data from the pilot case study to the actual case study, which might negatively influence its overall quality. Telephone interviews and/or personal interviews were conducted to collect data, using a reduced version of the constructed questionnaire. In detail, the interviews were carried out in eight subsystems of the analysed defence supply chain (including customer (overseas), Bundeswehr Logistics Centre, depot, collective depot; see figure 5) by two researchers each, and with one contact person.

During data collection, the principles recommended by Yin (2009) have been applied (cf. Yin, 2009). The involvement of several researchers during the data collection phase – in terms of the so-called investigator triangulation – helps to avoid, or significantly reduce, the risk of subjective bias (Denzin, 1978). Moreover, a database was established documenting all data material gathered in the course of the pilot case study. Finally, data emerging from the interviews served to maintain a chain of evidence. Due to the consideration of these three principles, it was possible to positively influence reliability as well as construct validity, thus enhancing the quality of the overall case study (Yin, 2009).

Data analysis

The following phase of data analysis was carried out applying the strategies of within-case and cross-case analysis (Miles/Huberman, 1994). Within-case analysis was used so as to achieve a deeper understanding of each subsystem of the defence supply chain (Eisenhardt, 1989). Therefore, in the course of the empirical investigation undertaken here, two steps are distinguished: Firstly, for each subsystem, a FMEA sheet (as described in the phase of preparation) was created comprising the identified and assessed (with respect to the determinants D, O, and S) risk factors. Based on this, a risk map was created in order to be able to better compare the respective risk factors. Secondly, the focus of the subsequent cross-case analysis was on the comparison of the individual subsystems (Eisenhardt, 1989). In concrete terms, in the course of the empirical investigation, the identification of patterns between the subsystems was to be considered the primary objective. By applying this analytical technique, the conclusion could be drawn that the character of certain risk factors (e.g., *Breakdown of the data processing centre*, reflecting a safety-related process risk within the defence supply chain) was perceived similarly by the respective subsystems. Thus, such risk factors could be seen as typical defence supply chain risks (cf. figure 7). In consequence, it was possible to perform a classification of relevant and less relevant risk factors which prevail at the defence supply chain level.

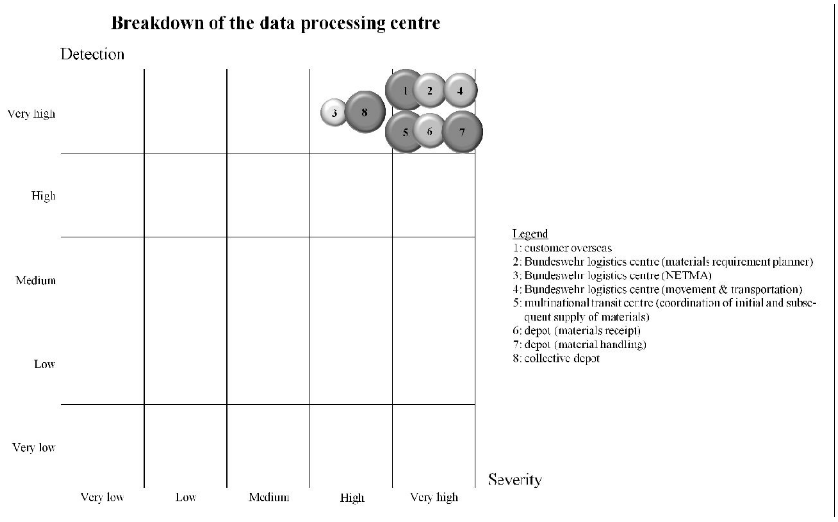

Figure 7: Defence supply chain risk map using the safety-related process risk *Breakdown of the data processing centre* as an example.

RESULTS

With the creation of the case study report (for a detailed overview of its elements see Stake, 1995), the pilot case study was completed. Apart from its common elements, the report provided important insights, among others:

- The analysed defence supply chain is currently characterised by a low effectiveness. This is expressed by the fact, that a high number of safety- and security-related risk factors distributed across the respective risk categories have been confirmed that adversely affect its continuity of supply. What is remarkable, in particular, is the low probability of detection which applies to all institutions for a variety of the statements formulated in the questionnaire. This is mainly attributed to the missing overlap of detection and occurrence of a risk factor in terms of time and space. Instead, its detection takes place downstream in the defence supply chain. At this point the statement *Data get lost* should be mentioned as an example. This factor, if any, will be detected by the institution concerned on an informal basis – e.g., by means of a phone call made by the institution waiting for the data.
- Moreover, the analysed defence supply chain is currently characterized by a low efficiency. This is expressed by the fact, that

there is a substantial unused potential for cost minimisation in terms of saving money in the defence supply chain. For example, goods requested by the military end customer located in the operational area are only ordered after stocks have been completely exhausted. Consequently, to limit the time between order and supply, to more than 90% goods are delivered by air transportation which is the most expensive type of transport. The resulting renunciation of alternative, more cost-effective types of transport, such as rail, road, or sea can be deemed a huge potential for cost minimisation.

- The existing risk factors result to a high degree from a lack of overall coordination of the actors of the defence supply chain. This is attributed, in particular, to the lack of understanding of SCM. In principle, no institution has confirmed the statement *Knowledge of the institutions upstream and downstream in the defence supply chain does not exist*. However, the creation of isolated applications becomes apparent. The interface $customer_{overseas}$ is characterised by an extreme fluctuation. Each contingent of troops located in the operational area is being automatically replaced approx. every four months by another one. According to the results generated in the course of the pilot case study the following conclusions can be drawn: The interface 1 and 19, respectively, is distinguished by an insufficient handing over (e.g., in terms of outstanding deliveries) and by a lack of interest of the individual contingents of troops for each other (e.g., in terms of releasing orders for succeeding contingents of troops at an early stage). Then, possible consequences are, for example, to release an order twice, or temporarily not be able to maintain the continuity of supply due to a lack of goods. This in turn has a negative effect on the efficiency, and on the effectiveness respectively, of the analysed defence supply chain.
- Finally, the risk factors resulting from the leagile character of the defence supply chain should be emphasized. Thus, a lack of understanding for the different conditions prevailing between basic logistics and logistics support operations has implicitly as well as explicitly emerged from the pilot case study conducted here. This assumption is reflected by the different objectives pursued by the individual institutions. The focus of the $customer_{overseas}$ is on the continuity of supply (i.e., ensuring effectiveness). In this context, the labelling of the orders released by the $customer_{overseas}$ with the constantly highest possible priority can be considered one safety- and security-related risk factor – this does, in fact, not only hamper an actual distinction between more and less urgent goods. Moreover, this impacts the type of transport to be chosen (air transportation) and the

related increase in costs. By constrast, the focus of the procurement organisation is on the minimisation of costs (i.e., ensuring efficiency). The emerging risk factor is to be seen in the partial quantitative and/or qualitative modification of the orders released by the $customer_{overseas}$ which possibly can't be used and which, therefore, do not contribute to the continuity of supply.

To summarize, it is not only the results exemplarily discussed here that show the need for further examination in the form of a more comprehensive case study. Rather, it is also the actors of the analysed defence supply chain who are strongly in favour of such a follow-up study.

DISCUSSION

The aim of this paper was to develop a conceptual framework for an armed forces-specific SCM. In this context, defence supply chain structures, processes, and strategies have been analysed and the relevance of integrating safety- and security-related aspects by means of a specific management component has been highlighted. Based on this, the SCSM approach was introduced, the objective of which is ensuring continuity of supply (i.e., effectiveness) in supply chains while also taking the economic goal of profitability (i.e., efficiency) into consideration. The subsequent empirical investigation has revealed the need to adapt SCSM as an appropriate management component in defence supply chains. On the one hand, risk factors have been identified which have a negative effect on the safety, and on the security of the defence supply chain respectively. On the other hand, risk factors have been identified which have a negative effect on the effectiveness, and on the efficiency respectively. Thus, since the SCSM aims at both ensuring the continuity of supply and minimising costs, the need to take into consideration this approach has been demonstrated. Further research would need to include an expansion of the pilot case study, considering the defence supply chain as a whole, and implementing the entire strategic planning process.

REFERENCES

Bertsche, B. (2008). "Reliability in automotive and mechanical engineering." Berlin, Heidelberg: Springer.

Billington, C. (2002). "HP cuts risk with portfolio approach." *Purchasing*, 131(3): 43.

Bowersox, D.J. (1997). "Integrated Supply Chain Management: A Strategic Imperative." *Annual Conference Proceedings*, Council of Logistics Management fall meeting, Chicago: 181-189.

Boyne, G.A. (2002). "Public and Private Management: What's the Difference?" *Journal of Management Studies*, 39(1): 97-122.

Bundesministerium der Verteidigung (2004). "Grundzüge der Konzeption der Bundeswehr." Berlin.

Bundesministerium der Verteidigung (2001). "Teilkonzeption Logistik." not published document, Berlin.

Byrne, B. (2009). "Structural Equation Modeling With AMOS: Basic Concepts, Applications, and Programming." 2nd edition, New York, Hove: Routledge Academic.

Christopher, M. (1998). "Logistics and Supply Chain Management – Strategies for Reducing Cost and Improving Service." 2nd edition, London: Financial Times.

Christopher, M./Peck, H. (2004). "Building the Resilient Supply Chain." *The International Journal of Logistics Management*, 15(2): 1-14.

Christopher, M./Peck, H./Towill, D. (2006). "A taxonomy for selecting global supply chain strategies." *The International Journal of Logistics Management*, 17(2): 277-287.

Christopher, M./Towill, D.R. (2000). "Supply chain migration from lean and functional to agile and customised." *Supply Chain Management: An International Journal*, 5(4): 206-213.

Commission of the European Communities (2007). "Commission staff working paper: Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on the coordination of procedures for the award of certain public works contracts, public supply contracts and public service contracts in the fields of defence and security - Summary of the Impact Assessment {COM(2007) 766 final} {SEC(2007) 1598}." Brussels.

Cooper, M.C./Lambert, D.M./Pagh, J.D. (1997). “Supply Chain Management: More Than a New Name for Logistics.” *The International Journal of Logistics Management*, 8(1): 1-14.

Craighead, C.W./Blackhurst, J./Rungtusanatham, M.J./Handfield, R.B. (2007). “The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities.” *Decision Sciences*, 38(1): 131-156.

Denzin, N. K. (1978). “The Research Act in Sociology: A Theoretical Introduction to Sociological Methods.” 2nd edition, London: Butterworths.

Deutch, J. (2002). “Assessment of the Security Threat.” In Rice, J. B. (ed.), *Supply Chain Response to Terrorism – Planning for the Unexpected* (pp. 1-2). [On-line]. Available at http://web.mit.edu/supplychain/repository/scresponse_120502v1.pdf, [Retrieved March 8, 2010].

Dorobek, S./Eßig, M./Klein-Schmeink, S. (2009). “Besonderheiten öffentlicher Wertschöpfungsketten: Herausforderung für die Konzeption der Öffentlichen Logistik.” In Eßig, M./Witt, M. (eds.), *Öffentliche Logistik: Supply Chain Management für den öffentlichen Sektor* (pp. 151-196). Wiesbaden: Gabler.

Egger, E. (1992). “Datenschutz und Datensicherheit – Grundlagen oder Spezialgebiet?” *Datenschutz und Datensicherung*, 16(10): 512-516.

Eichhorn, P. (2001). “Öffentliche BWL als eine Spezielle BWL.” *Wirtschaftswissenschaftliches Studium*, 30(8): 409-416.

Eisenhardt, K.M. (1989). “Building Theories from Case Study Research.” *Academy of Management Review*, 14(4): 532-550.

Ellram, L.M. (1996). “The Use of Case Study Method in Logistics Research.” *Journal of Business Logistics*, 17(2): 93-138.

Ellram, L.M./Birou, L.M. (1995). “Purchasing for Bottom Line Impact: Improving the Organization through Strategic Procurement.” Chicago: McGraw-Hill.

European Commission (2009). Defence Procurement. [On-line]. Available at http://ec.europa.eu/internal_market/publicprocurement/dpp_en.htm, [Retrieved March 9, 2010].

Federal Ministry of the Interior (2005). Protection of Critical Infrastructures – Baseline Protection Concept. [On-line]. Available at http://www.bmi.bund.de/cae/servlet/contentblob/121746/publicationFile/

13193/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf, [Retrieved March 8, 2010].

Fisher, M.L. (1997). "What is the right supply chain for your product?" *Harvard Business Review*, 75(2): 105-116.

GG (2009). "Grundgesetz für die Bundesrepublik Deutschland (GG) vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Artikel 1 des Gesetzes vom 31. Juli 2009 (BGBl. I Nr. 48 S. 2248)."

Hartley, K. (2006). "Defence Economics." Discussion Paper, Centre for *Defence Economics*, University of York, 2006.

Hartley, K. (2002a). "Defence Economics: Its Contribution and New Developments." Centre for *Defence Economics*, University of York, 2002a.

Hartley, K. (2002b). "The Economics of Military Outsourcing." *Public Procurement Law Review*, 11(5): 287-297.

Hofstetter, J.S./Stölzle, W. (2009). "Outsourcingpotentiale in der Schweizer Armee." In Eßig, M./Witt, M. (eds.), *Supply Chain Management für den öffentlichen Sektor* (pp. 197-230). Wiesbaden: Gabler.

Hogg, M.A./Vaughan, G.M. (2008). "Social Psychology." 5th edition, Essex: Prentice Hall International.

Jüttner, U./Christopher, M./Godsell, J. (2006). "Demand Chain Alignment – Understanding the Capability underlying effective Product Lifecycle Management." *Industrial Marketing Management*, 35(8): 989-1001.

Lai, E.M. (2003). "An Analysis of the Department of Defense Supply Chain: Potential Applications of the Auto-ID Centre Technology to improve Effectiveness." Massachusetts.

Lambert, D.M./Cooper, M.C. (2000). "Issues in Supply Chain Management." *Industrial Marketing Management*, 29(1): 65-83.

Lambert, D.M./Emmelhainz, M.A./Gardner, J.T. (1996). "Developing and Implementing Supply Chain Partnerships." *The International Journal of Logistics Management*, 7(2): 1-17.

Lambert, D.M./García-Dastugue, S.J./Croxton, K.L. (2005). "An Evaluation of Process-oriented Supply Chain Management-Frameworks." *Journal of Business Logistics*, 26(1): 25-51.

Lange, J.A. (2005). “Sicherheit und Datenschutz als notwendige Eigenschaften von computergestützten Informationssystemen: Ein integrierender Gestaltungsansatz für vertrauenswürdige computergestützte Informationssysteme.” Wiesbaden: Deutscher Universitäts-Verlag/GWV Fachverlage GmbH.

Large, R. (2006). “Strategisches Beschaffungsmanagement: Eine praxisorientierte Einführung.” 3rd edition, Wiesbaden: Gabler.

Lee, H.L./Wolfe, M. (2003). “Supply chain security without tears.” *Supply Chain Management Review*, 7(1): 12-20.

Lewis, J.P./Dudley, R.E. (2005). “The McGraw-Hill Guide to the PMP Exam.” New York: McGraw-Hill.

Marshall, C./Rossman, G.B. (1995). “Designing Qualitative Research.” 2nd edition, Thousand Oaks: SAGE Publications, Inc.

Mathaisel, D.F.X./Manary, J.M./Comm, C.L. (2009). “Enterprise Sustainability: Enhancing the Military’s Ability to Perform Its Mission.” Boca Raton: CRC Press.

Matschke, K.-D./Ick, R. (1998). “Security Quality Management Handbuch: Grundsätze und Verfahren für umfassende Unternehmenssicherheit.” Ingelheim: SecuMedia.

Mentzer, J.T./DeWitt, W./Keebler, J.S./Min, S./Nix, N.W./Smith, C.D./Zacharia, Z.G. (2001). “Defining Supply Chain Management.” *Journal of Business Logistics*, 22(2): 1-25.

Metz, P.J. (1997). “Demystifying Supply Chain Management: Accomplishments and Challenges.” Annual Conference Proceedings, Council of Logistics Management fall meeting, Chicago, 237-255.

Miles, M./Huberman, A.M. (1994). “Qualitative Data Analysis: An Expanding Sourcebook.” London: Sage Publications, Inc.

Naylor, J./Naim, M./Berry, D. (1999). “Leagility: integrating the lean and agile manufacturing paradigms in the total supply chain.” *International Journal of Production Economics*, 62(1-2): 107-118.

Neher, A. (2005). The Configurational Approach in Supply Chain Management.” In Kotzab, H./Seuring, S./Müller, M./Reiner, G. (eds.), *Research Methodologies in Supply Chain Management* (pp. 75-89). Heidelberg, New York: Physica-Verlag HD.

North Atlantic Treaty Organization (2007). NATO Logistics Handbook. [On-line]. Available at http://www.nato.int/docu/logi-en/logistics_hndbk_2007-en.pdf, [Retrieved March 8, 2010].

Oliver, R.K./Webber, D. (1982). "Supply chain management: logistics catches up with strategy." In Christopher, M. (ed.), *Logistics – The Strategic Issues* (pp. 63-65). London, New York et al.: Chapman & Hall.

Patton, M.Q. (1990). "Qualitative Evaluation and Research Methods." 2nd edition, Newbury Park: Sage Publications, Inc.

Rice, J. B./Caniato, F./Fleck, J./Disreally, D./Lowtan, D./Lensing, R./Pickett, C. (2003). "Supply Chains Response to Terrorism: Creating Resilient and Secure Supply Chains." Supply Chain Response to Terrorism Project, Interim Report of Progress and Learning, MIT Centre for Transportation and Logistics, Massachusetts.

Rogers, D. (1981). "Managing in the public and private sectors: Similarities and differences." *Management Review*, 70(5): 48-54.

Sheffi, Y./Rice, J.B./Fleck, J.M./Caniato, F. (2004). "Supply Chain Response to Global Terrorism: A Situation Scan." Conference Proceedings, University of Milan, "Supply Chain Conference", Milan.

Shewchuk, J.P. (1998). "Agile manufacturing: One size does not fit all." In Bititci, U.S./Carrie, A.S. (eds., 1998), *Strategic Management of the Manufacturing Value Chain* (pp. 143-150). Norwell, Dordrecht: Springer.

Simchi-Levi, D./Kaminski, P./Simchi-Levi, E. (2000). "Designing and Managing the Supply Chain: Concepts, Strategies, and Case Studies." Boston: McGraw-Hill/Irwin.

Stake, R.E. (1995). "The art of case study research." Thousand Oaks: Sage Publications, Inc.

Steiner, G.A. (1969). "Top Management Planning." London: Macmillan.

Steven, M./Tengler, S. (2005). "Informationssicherheit im Supply Chain Management." *Wirtschaftswissenschaftliches Studium*, 25(6): 345-348.

Stockholm International Peace Research Institute (2009). SIPRI Yearbook 2009. Armaments, Disarmament and International Security – Summary. [On-line]. Available at http://www.sipri.org/yearbook/2009/files/SIPRIYB09summary.pdf [Retrieved March 8, 2010].

Supply Chain Council (2008). Supply Chain Operations Reference model, Overview Version 9.0. [On-line]. Available at http://www.supplychain.org/f/SCOR%2090%20Overview%20Booklet_0.pdf, [Retrieved March 8, 2010].

Tatham, P. (2005). “Efficient in Peace but Effective in War: Meeting the Challenge of the Military Supply Chain – An Agenda for Research.” Supply Chain Practice, 7(2): 42-57.

Vonderembse, M.A./Uppal, M./Huang, S.H./Dismukes, J.P. (2006). “Designing supply chains: towards theory development.” *International Journal of Production Economics*, 100(2): 23-38.

Yin, R.K. (2009). “Case Study Research: Design and Methods.” 4th edition, Thousand Oaks: Sage Publications, Inc.