

Port and Maritime Security: A Critical Analysis of Contemporary EU Policies

A. A. Pallis and G. K. Vaggelas

Department of Shipping, Trade and Transport, University of the Aegean.
Email: apallis@aegean.gr ; g.vaggelas@stt.aegean.gr

Abstract

In recent times, European Union (EU) policies aiming to promote the competitiveness of European ports and their integration in supply chains have been complemented by the discussion of regulatory initiatives aiming to minimize risk and increase the security and operational reliability of the sector. This paper analyses the operational and economic implications of the enactment of these EU policy measures for ports. In this vein, it also discusses the major controversies that have arisen between policy-makers and stakeholders as regards the introduction of further supranational policies. A long-term strategy with a reference to all parts of the supply chain is under consideration. Whilst the aim of all these EU policies is to introduce security standards for (trans)port service providers, they also affect Europe's ports in several economic and operational ways. Among the issues to be discussed in this paper are the resulting task division between port authorities, other relevant authorities, and stakeholders; the cost implications of these measures for the various actors; the search for a balance between risk and regulatory policies; and the emerging financial issues in order to enhance security by the enactment of the EU to maintain a balanced level playing field.

Keywords

Port and maritime security; European port policies; Economics; operations.

1. Introduction

Transport security has become a vital issue worldwide and a new scene has revealed: security of the whole supply chain, including ports, has been transformed into a key theme of public port policies. Related regulations have been introduced at three levels: national level, for example the USA; peripheral/supranational, for example the EU; and international level, for example the International Maritime Organisation (IMO). The ultimate purpose of these policies is to minimize the security risk thus preventing unlawful acts that may occur throughout

the transportation chain.

Maritime security is the resistance to an intentional, unauthorised act designed to cause harm or damage to ships and ports. This definition can also be extended and applied to the entire supply chain. A broad, yet major, distinction between safety and security is that security has a reference to the protection from intentional acts, while safety has a reference to the protection from accidental events.

Security risk in transport equals to the combination of two factors. The first factor is the vulnerability of the system, which reflects the possibility of a successfully undertaken unlawful act against the transport network compared to the possibility of protecting it through inherent or managed safeguards. The second factor is the consequences of such a successfully undertaken unlawful act. These consequences are related to two measurable magnitudes, the possible number of fatalities and the economic impact of these acts respectively. The latter is calculated in relation to the reconstruction costs, the disruption time of the transport flow, and the volume of transport flow.

The introduction of security measures in the international transportation process has greatly influenced the competitiveness of modes and supply chains. In combination with factors such as cost, time, safety and risk, security has become a factor affecting the competitive position of all the supply chain related stakeholders. Therefore, questions regarding which market actors should act in order to enhance the security of the system and how should they do so, as well as who should bear the cost of security implication, are vital.

Following the events of 9/11, the European Union (EU) policy-making institutions advocated a port security 'policy gap' and moved decisively towards developing regulatory and non-regulatory initiatives aiming to minimize risk and increase the security and operational reliability of the sector.

Since the early 1990s, the focus of port policies in Europe had been on restructuring the port industry and reinforcing the quality of provided services, i.e. by integrating ports in supply chains (Pallis and Chlomoudis, 2002). Progressively (Psaraftis, 2005; Pallis, 2007) these efforts have been accompanied by the search for a

collective public policy regime that would ensure secure port operations for all international European ports.

Some EU policy initiatives have already been transformed into EU laws, while other proposals, like the draft regulation on supply chain security, are still under discussion. A long-term strategy with a reference to all parts of the supply chain was put forward by the European Commission in the form of a Green Paper on a European programme for critical infrastructure protection (CEU, 2005a) and is currently under consideration by policy-makers and stakeholders. A specific policy on maritime infrastructure protection is under preparation. Whilst the aim of all these policies is to introduce security standards for (trans)port service providers and the secure operator concept, they also affect Europe's ports in several economic and operational ways.

This paper presents the EU security related initiatives affecting European ports and analyses the implications of their enactment. It also discusses the major controversies as regards the introduction of further supranational policies. Some of the other issues examined in an effort to enhance security while maintaining a balanced level playing field for all EU ports include the resulting task division among port authorities, other relevant authorities and stakeholders, the cost implications of these measures for the various actors, the search for a balance between risk and regulatory policies and the emerging financial issues.

Section 2 investigates the rationale behind the recent transformation of security into a primary issue in transport related public policies, while Section 3 focuses on the main international and national mandatory or voluntary security regulations and initiatives that are closely related with the content of the relevant EU policy initiatives. The relevant EU policies are analysed in Section 4, which concludes with the presentation of the perspective of the various stakeholders on the implications of the existing and under discussion relevant policies. Section 5 closely looks at the costs and the benefits of the security related EU rules. The concluding section has a reference to the potential future policy directions.

2. Port Security as a Major Public Policy Issue

A few years ago the enhancement of port and supply chain security was not a major policy issue. Nor was it treated as a necessary factor to be tackled by the companies involved in trade and transport. International organisations occasionally adopted security guidelines. This pattern had developed despite the fact that, national security regulations, whenever existing, encountered several implementation difficulties due to their spatial dimension: by concerning only specific transport processes, or even some specific infrastructures, their implementation did not cover all the potential targets of unlawful acts.

The driving forces inducing the reversal of the trend towards international decision-making and the way in which security is treated are three. The first one is the increased frequency of unlawful acts that took place at economic centres and/or transport nodes. The second

driving force is the spatial dimension of security related regulations. The limited spatial jurisdiction of national policies hampered their potential to turn to a holistic approach of tackling security issues in transport and global trade systems. The third driving force concerns the structural changes of world economy and the implementation of advanced technologies, which altered the way transport systems in general, and ports in particular, operate. Focusing on the EU this list of parameters should also include the economic importance of the port sector for the European economy.

Nowadays, security is a global issue affecting the entire transport sector. Acting internationally, public agencies introduced a number of regulatory and non-regulatory measures in order to enhance it. The September 2001 World Trade Centre, New York attacks, accelerated work on coherent security measures in maritime transport at international level. Fearing that ships could carry weapons of mass destruction or be used as weapons themselves, member governments of the International Maritime Organisation (IMO) met in December 2002 to establish mandatory security standards for ships and ports.

Unlawful acts disrupting maritime transport activities and endangering lives onboard are not a new phenomenon. The hostage of passengers onboard the cruise ship *Aquile Lauro* (October 1985) is just an example. Unfortunately however, since 2000 the frequency of such actions has increased. Maritime related incidents, like the attacks on the battle cruiser *USS Cole* (October 2000) outside the harbour of Aden, and the oil tanker *MV Limburg* (October 2002), were not the only ones. Other transport modes were also affected, including the Madrid commuter trains (March 2004) and the London public transport system (July 2005), with these unlawful acts taking place in the aftermath of the September 2001 events.

All the above indicated the vulnerability of the different transport modes to unlawful acts. National governments and international organisations responded by a fast-track endorsement of policy initiatives, reflecting a changing geopolitical climate. After the attacks at the WTC, security moved up on the political agenda.

The European Commission addressed the issue of security in the White Paper drawing the themes of the EU Transport Policy up to 2010 (CEU, 2001), which was published just one day after the WTC attacks. However, this was a reference only to the security of passengers on board cruise vessels and ferries, as well as the security during the transportation of nuclear goods. The purpose of this reference was to cover only a limited part of maritime transport.

Gradually, the maritime security agenda expanded to include measures that minimise a number of security risk factors that are associated with cargoes (for example the potential to be used as weapons), vessels (the potential to be used to disrupt infrastructure and/or as weapons), and people (the potential transportation of people attacking ships or infrastructure), and limit the potential of transport means and nodes from becoming potential targets (Johnston, 2004).

Meanwhile, ports were affected by major economic, technological and organisational changes. Following the rapid and pervasive restructuring of supply chains and logistics pathways, modern ports are not simply places that facilitate the interface of sea and inland transport modes. Ports are areas of commercial, industrial and distribution activities (Barton and Turnbull, 2002), which are embedded in value-driven chain systems (Robinson, 2002). The expanding use of combined transport (cf. Slack, 1998) advanced this trend to an extent that was acknowledged by policy makers: EU institutions indicated the beginning of a new intermodal era for ports in the early search for a long-term EU port policy (see: CEU, 1997). At a latter stage, they endorsed public policies aiming to integrate ports in the multimodal transport chain (for details: Chlomodis and Pallis, 2002).

These developments produced the expansion of port hinterlands and port 'regionalisation' (Notteboom and Rodrigue 2005): there is a geographical and functional integration of ports in wider regions in order to serve a specialised transportation context by using the comparative advantage of spatially effective fragmented locations (i.e. better access to space, markets, labour, parts and resources). The concept of within port localisation, either for operational, and/or cost minimisation justifications, is downgraded. Complex transport flows and spatially fragmented operational networks operate as integrated systems, with a number of actors involved within the wider supply chain, operating on a wider geographical scale.

Ports integration in supply chains has certain security implications. By expanding the spatial area within which transport operations take place and due to the fact that intermediate goods are processed at various stage of the transport chain (cf. Juhel, 1998), one needs to secure the entire 'process' which begins at the manufacturing site, rather than the parts of the supply chain.

In Europe this process involves more than 4 million operators and is generally marked by low levels of security awareness. The fact that these complex networks are mostly situated near urban areas, adds to the necessity of approaching security issues through holistic frameworks (i.e. addressing the security of the entire chain), rather than piecemeal ones (i.e. addressing security in a specific transport mode or location). At the same time, the implementation of security measures at ports is a difficult task given the different priorities of the various stakeholders and the emerging multiplicity of port organisation and ownership statuses.

The economic importance of the port sector for the EU stands as an additional driving force for developing European-level policies aiming to address security concerns. A total of 3,5 billion tons of cargo (90% of the external EU trade and the 40% of the intra-EU trade) and 350 million passengers are annually transported via European ports. Ports are also significant as places of employment and as added-value generators. The EU has approximately 1.200 seaports and 3.700 port facilities and including the services related to them, they produce an annual added value of 20 billion euros and employ

approximately 350.000 citizens.

3. Non-EU Maritime Security Initiatives

The USA have been the leading force for the introduction of a new maritime security regime. This is due to the the events that took place in 2001 and the wider geopolitical developments. Although developed in a non-EU context, these port security initiatives have had a considerable impact on the observed upgrade of the EU interest in developing its own policies. Two of the major maritime transport related security regulations with a global impact developed in the US and deal with container transportation.

The first of these regulations was the Container Security Initiative (CSI). This initiative has established relevant inspections of containers at the foreign ports where imports are loaded for the US, rather than at the US port of discharge. Today US customs officials are located in a number of these ports around the world from which the vast majority of containerised US imports is transported. CSI is implemented on a reciprocal basis, allowing participating countries to send their customs officers to major US ports in order to inspect containerised cargo being exported to their countries (CBP, 2006a).¹

The CSI has certain implications beyond the USA, especially as, since January 2003, its implementation goes hand-in-hand with the application of the '24-hour rule'. According to the latter, the US Customs and Border Protection Agency must receive cargo manifest information and bills of lading information from carriers, 24-hours before cargoes bound for the US are loaded on-board ships departing from a foreign port. The 24-hour rule has generated concerns for potential distort of port competition worldwide (cf. UNCTAD, 2004) since some ports might gain the status of more favourable origins for seaborne trade towards the US than others. CSI also contains measures for the elimination of crew list visas, trying to discourage foreign seamen from embarking on ships from US ports, as a means to minimize potential security threats.

This process shifts costs to foreign shippers and ports (CBP, 2006b) and generates policy developments outside the US. To secure container trade according to an 'acceptable' CSI regime, a bilateral US-EU agreement provides for joint customs cooperation (CEU, 2004a). This agreement indicates that at least some of the US security measures have a cost and operational impact on European supply chains (see: CEU, 2006a)

The Customs-Trade Partnership Against Terrorism (CTPAT) is the second major US security related initiative. According to this voluntary programme, the participating US importers impose security requirements on themselves and their partners in the supply chain with the ultimate goal being to secure the entire chain. This is an initiative operating on a voluntary basis with participants enjoying specific benefits as a motive for joining it. The most important one is the Green Lane award

¹ Two examples of countries that have sent customs officers to US ports are those of Canada and Japan.

according to which, Green Lane awarded operators are exposed to less customs inspections and consequently, decreased clearness time for cargo and customs procedures in US ports.

As in the case of maritime safety, some of the most important regulations regarding security in trade and transport have been undertaken by IMO. By the end of 2002, IMO had adopted a major security related amendment to the Convention of Safety Of Life At Sea (SOLAS). This is the new Chapter XI-2 that contains the International Ship and Port facility Security (ISPS) Code, a policy that was to change the way ship and port security is considered.

The ISPS Code has two parts. Part A is mandatory for all the contracted countries, while Part B contains recommended actions (some countries have adopted the second part as mandatory). The ISPS Code established three security levels denoting the need for normal (Level 1), heightened (Level 2), and exceptional (Level 3), security measures respectively. The implementation of the Code's requirements and the respective certification of vessels and shipping companies is the responsibility of the flag state, while ports' national authorities are responsible for inspecting, and certifying proper implementation. These provisions cover all types of ships that are bigger than 500 grt, mobile offshore drilling units, and port facilities serving ships, which are engaged in international voyages².

As regards ports, the ISPS Code concentrates on the locations of ship/port interface. Ports have to develop a Port Facility Security Plan (PFSP), detailing the actions that must be taken to prevent, or to correspond to, a security incident at this interface. They also have to designate a port facility security officer responsible for carrying out regularly drills, exercises and seminars in relation to port facility security. In addition, Part A makes an explicit reference to the 'identification and estimation of important assets and infrastructures that are important to protect'. This reference provides the background for the ongoing European search for a long-term programme that will effectively protect the critical maritime infrastructures in the EU.

Finally, the amended SOLAS Chapter XI-2 introduced a new technological security measure for ships. This is the Automatic Identification System (AIS), which enables ships to transmit a unique identification signal in order for the shore operational centres to observe the ship route. Ships are also required to have on board a security alert system transmitting a security alert to a designated competent authority when activated in emergency situations, and the Continuous Synopsis Record (CSR) that contains details of the ship (i.e: name, flag, port of registry, IMO number, and owner information).

The *Code of Practice on security in ports* is another security related initiative that has been undertaken by IMO jointly with ILO. This Code of Practice provides a guidance framework for the development of a strategy

appropriate to identifying threats to security in ports (IMO & ILO, 2003). The main provisions are:

- The development of a ports' security policy statement by the signatory states;
- The establishment of a Port Security Assessment;
- The identification and evaluation of the critical assets and infrastructures that are important to protect;
- The development of a Port Security Plan, compatible with the ISPS Code for a Port Facility Security Plan;
- The increased security awareness of personnel training.

Various other organisations strived to create security rules and related documentation. An example is the International Organization of Standardisation and its ISO series: *ISO 20858* provides guidelines on maritime port facility security assessment (ISO, 2004). *ISO 28000* gives guidelines on security management of supply chains (ISO, 2005), and *ISO 28001* gives specifications on best practices for implementing supply chain security (ISO, 2006).

A second example is the adopted in 2003 ILO *Revised Seafarer's Identity Documents Convention (No 185)* that establishes a 'positive' and 'verifiable' uniform global identity document for seafarers (ILO, 2003). The World Customs Organization adopted in 2004 a *Resolution on Security and Facilitation measures concerning the International Trade Supply Chain* (WCO, 2004). The latter requires from customs administrations to develop an action plan and cooperative arrangements between customs and the industry in order to increase the security of the trade supply chain.

Overall, security issues today are among the major policy-makers' concerns. The transboundary character of maritime flaws leads, almost mechanistically, to a growing number of global policy responses that respect this international character.

4. EU Security Policies

International policy developments took place in a period that the EU was reviewing its Common Transport Policy (CTP) strategy. In line with them, the relative White Paper identified the security of (maritime) transport systems and passengers onboard cruise ships and ferries, as major issues that EU policies should address (CEU, 2001). In the same period, the Commission considered the bilateral agreements on CSI signed by EU member-states (Italy, France, Netherlands, Belgium, Germany) powerless to reverse situation and limit security related worries.

Since then, the EU has been a leading policy-maker in the field. In its Declaration, the European Council of March 2004 called for the strengthening of the security of all forms of transport, through the enhancement of the legal framework and the improvement of prevention mechanisms. The reaction of the Commission was to decisively co-ordinate European reactions, initially by producing proposals based on the IMO agreements, and then focusing on related issues of competence (cus-

² The EU and South Africa are among those that have expressed the intention to extend the ISPS Code to special ships bigger than 500gt, such as research, expedition and survey vessels, training vessels, and fish factory ships.

toms), competition (between ports), external relations and integrated security measures.

Reversing a long period of inertia (cf. Power, 1992; Pallis, 2002) the EU developed a rather comprehensive regional regulatory framework in order to secure trade and transport systems. It did so via an evolutionary process, which reflects the endorsement of the concept that the realities of the market make a “big bang” approach unrealistic.

4.1 Enhancing Ship and Port Facility Security

The EU adopted a Regulation mainly aiming at transposing the provisions of the ISPS Code and the rest of the SOLAS amendments into binding EU law.³ The scope is to reinforce a comprehensive and uniform implementation of the mandatory requirements of the ISPS Code throughout the Union,

Regulation 725/2004 (and the ISPS Code) requires that ship and port facility security plans (SSPs and PFSPs) specify a range of security measures to be maintained by ships and port facilities. Ports have to identify restricted areas and monitor them in order to prevent unauthorised access, and implement measures to prevent weapons, dangerous substances and devices being taken onto ships or into port facilities.

While the ISPS covers ships engaged in international voyages and those ports that accommodate them, Regulation 725/2004 includes provisions that extend these measures to the ships engaged in national voyages within the EU, as well as the related port facilities that serve these ships. It also introduces a different agenda by extending the application of the rule to a certain extent to domestic traffic of member-states (i.e. to those ports that might only occasionally serve international transport). The specified port area that is covered by this Regulation is ‘the location where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from sea ward as appropriate. This designation of the port area that must be secured is the same as in the ISPS Code.

This rule also requests member states to identify and evaluate the transport assets and infrastructure that are important to protect. The primary concern of this process is the avoidance of death or injury. The secondary concern is to figure out how the port facility, structure or installation can rapidly re-establish a normal functioning following the threat or occurrence of a security incident. Member states retain the power to determine further measures in order to ensure the appropriate level of security in port facilities that serve only occasionally international voyages, thus not covered by the ISPS Code. Finally the EU rule created an inspection regime that is managed, and ex-post monitored, by the Commission.

The ISPS Code has been implemented in European ports with international traffic since 2004. The absence of reports of security incidents of high risk levels in these ports suggests a general good situation of port

security. Yet several shortfalls have been recorded in EU ports and include the following:

- Cases of ships that insist on a Declaration of Security even though both the port and the vessel are at low security level, which is causing unnecessary trouble and work.
- Cases of vessels present tonnage certificates which claim a tonnage of 499 in order to be exempt from the Code.
- Problem of communication/information flows between different parties involved in the implementation of ISPS.

4.2 Revised Customs Code

In the aftermath of the endorsement of the CSI by the US in 2003, and the US-EU customs agreement to reciprocal practices in order to strengthen maritime container security in 2004, the EU adopted Regulation 648/2005, which details a revised EU custom code, in turn setting up common European secure custom systems⁴.

The revised customs code introduced measures to tighten security for goods entering or leaving the EU. The measures, which will be fully in force in 2009, aim to produce better-targeted customs controls, and be consistent with the analysis and electronic exchange of risk information between customs authorities in a common risk management framework. This policy follows the principles of the US C-TPAT regulation and similarly to the 24-hour rule, it sets up risk-based controls by establishing the requirement of pre-arrival or pre-departure information for all goods brought into or out of the customs located in the EU territory.

It also introduces for the first time, the status of the Authorized Economic Operator (AEO) as a core element for enhancing supply chain security. When an operator complies with the administrative rules and supply chain security requirements, as defined by the code, he is awarded the AEO status and experiences reduced customs inspections; a status similar to the Green Lane award that is established in the US under the C-TPAT regulation. There are four criteria to be fulfilled in order to be granted the AEO status:

- Appropriate record of compliance with customs requirements;
- A satisfactory system of managing commercial records;
- Proven financial solvency (where appropriate);
- Appropriate security and safety standards (where applicable).

As a consequence of the requirements of the new customs codes in both sides of the Atlantic (i.e. C-TPAT and the EU revised Code), customs now fulfil a new upgraded role when a few years ago their major task was the collection of import duties. Now customs also have a tendency to become security inspectorates of imported and exported cargoes.

³ Regulation 725/2004, of 31 March 2004, on enhancing ship and port facility security, OJ L. 129/6, 29.4.2004.

⁴ Regulation 648/2005, of 13 April 2005, amending Council Regulation 2913/92 establishing the Community Customs Code. OJ L 117, 13–19, 4.11.2005.

4.3 Enhancing Port Security

Within this context, the EU discussed additional measures aiming explicitly to secure the port industry. As Regulation 725/2004 tackles the issue of security at the ship/port interface, the EU moved in order to secure the rest of the port. This led to the adoption of Directive 65/2005 on enhancing security in the broader port area, giving particular attention to RO/RO vessels carrying passengers and vehicles⁵. The latter depends on the boundaries of the port, and given the absence of a widely accepted definition of the 'port area', the directive leaves the designation of the port boundaries to the member-states. In turn, member states must comply with the directive requirements no later than June 2007.

Directive 65/2005 applies to every port in which one or more port facilities are situated to which the Regulation 725/2004 applies; thus an approved Port Facility Security Plan (PFSP) exists. Measures to enhance port security consist of common basic rules, an implementation mechanism, and an appropriate compliance monitoring system, with a clear division of tasks between the parties involved. Ports must develop a Port Security Plan (PSP) that contains the necessary procedures and actions to be undertaken in the event of a security incident.

The monitoring of the compliance, including the confidentiality and dissemination of information, has to be implemented by a responsible Port Security Authority established in each member state. Moreover, every port or, if necessary, a group of ports must have a Port Security Officer (PSO) who acts as the contact person. Finally, the Directive designates three security levels (normal, heightened, and exceptional) reflecting differences in the risk profile of different sub-areas in the port, and demands different measures. The whole process shall be revised at least once every five years, while member states have to ensure the presence of a focal point for port security assigned the role of contact point with the Commission, in order to ensure the proper implementation of the Directive.

This rule supplements Regulation 725/2004. By implementing security measures to the whole port, it contributes to the creation of a common playing field for the entire port sector. Second, Directive 65/2005 is in line with the view that only a uniform level of security at all ports will reduce the risk of disruption in global supply chains (Banomyong, 2005). Towards the reduction of this risk, the Commission has already proposed an additional regulation on supply chain security.

4.4 Supply Chain Security

Having addressed different transport modes and nodes with security related regulations⁶, the EU moved towards developing rules for the protection of the remaining parts of the supply chain. The absence of such rules contradicts the necessity for a holistic approach of secu-

rity and for the application of security measures to the entire supply chain in which ports are integrated (Bichou, 2004).

Supply chain management expands the principles of logistics management to customers and suppliers, crossing geographical and organizational boundaries (Henstra & Woxenius, 1999). On these grounds, the Commission proposed a Regulation in 2006 aiming at enhancing supply chain security (CEU, 2006a). A key theme is the integration of the various piecemeal EU initiatives and in order to do so, the proposal elaborates the concept of 'known shipper/operator' to the whole supply chain, making use of already existing concepts like 'authorised economic operator'. If adopted, this measure will affect the port industry, as supply chain corridors commence at the production site and end at the cargo's final point of destination.

The philosophy of the EU institutions is that 'any chain is only as secure as its weakest link'. The Commission has endorsed this concept since the consultation process of Regulation 725/2004. In this vein, its policy initiative recognises four groups of supply chain activities:

1. The preparation of goods for shipment and shipment from the production site;
2. The transportation of goods;
3. The forwarding of goods; and
4. Warehousing, storage and inland terminal operations⁷.

The security of the entire supply chain is feasible only in situations that each operator assumes responsibility for the security of his/her own activity. Towards this end the Commission proposes the method of 'positive discrimination'. According to the proposal in discussion, the various stakeholders will be motivated by the secure operator (SO) status, to be awarded to any supply chain operator that fulfils minimum security requirements. This status will be designated to an operator by the member-state in which it operates and will be recognised by all member-states. As in the case of the AEO status, the benefits include facilitations in security controls, and a quality status. Due to the latter, security performance might create a commercial and competitive advantage. The measure will contribute to the formation of a homogeneous security environment with common requirements, awareness and objectives throughout Europe.

During the consultation process however, stakeholders were critical of additional security measures in the field of maritime (and air) transport, arguing that any security rule addressing the supply chain has to include only provisions that complement existing policies. Transport operators reacted strongly on the proposed regulation supporting that the new measure would have a tremendous cost, affecting mainly the SME's, while the benefits would be minor. Within this context, the European Commissioner responsible for Transport decided on December 2006 to postpone developments and set a date for the reevaluation of the proposal in the beginning of 2008.

⁵ Directive 2005/65, of October 26, on enhancing port security, OJ L. 310/28, 25.11.2005.

⁶ For instance on December 16 2002, the EU adopted Regulation 2320/2002 establishing common rules in the field of civil aviation security". OJ L. 355, 30.12.2002.

⁷ For a description of the supply chain security requirements: DNV Consulting (2005).

4.5 Protection of the European Critical Infrastructure

In 2005 the EU embarked on a discussion about a European Programme for Critical Infrastructure Protection (EPCIP), aiming to cover the infrastructures that are vital for the EU (CEU, 2005a).

European critical infrastructures are those physical resources, services and information technology facilities, networks and infrastructure assets or parts thereof that if disrupted, or destroyed, would have a serious impact on critical social functions (including the supply chain, health, safety, security, economic or social well-being) of two or more member-states, or a single member-state if the critical infrastructure is located in another member state (DG-TREN, 2006a). Such critical infrastructures can be found in 11 sectors, one of them being transport.⁸

The EPCIP considers unlawful acts, as well as disasters due to natural phenomena. The goal is to ensure adequate and equal levels of protective security on critical infrastructures, minimal points of failure, and tested recovery arrangements, while at the same time minimise the negative impacts that increased security investments might have on the competitiveness of a particular industry. The three main steps towards this direction are: (a) the identification of the European critical infrastructures; (b) the assessment of their vulnerability and the needs for additional protection; and (c) the introduction whenever necessary, of additional protection measures.

For each EU member-state, this strategy implies the establishment of a Critical Infrastructure Protection Authority responsible for monitoring the process within this state. For the operator of the infrastructure, it implies the development of an Operator Security Plan, which describes the security measures that have been taken, and a security action plan in relation to the protected infrastructure. It also implies the designation of a Security Liaison Officer who is the contact point between the authority responsible for the critical infrastructure and the Critical Infrastructure Protection Authority of the member state.

European ports with international traffic facilitate the function of the single European market and therefore can be characterised as critical infrastructures. Yet this development is controversial: there are not clear-cut criteria to be used in order to include or exclude specific ports from a list of ports characterised as European critical infrastructures (cf. Pallis, 2007). Port authorities, for instance, have already expressed concerns that such a list might result in undesirable side effects in terms of port development, planning and competition (ESPO, 2006).

DG-TREN (2006a) proposed the use of three criteria as a means to overcome this difficulty, advocating that the combined presence of these criteria should result in including ports in the list of the European critical infrastructures:

- A threshold of total traffic volumes (with an option

to exclude shortsea shipping and passenger volumes);

- The origin or final destination of a fixed percentage of cargo that flows outside the country where the port is located;
- The location of alternative ports in proximity to the port which will be able to handle equivalent volumes of cargo/passengers in order to substitute the port in the case of a terrorist attack.

However, several member states support the characterisation of all European seaports as 'critical'. ESPO demands the application of precisely the same criteria that apply for the inclusion of ports in the TEN-T. The reaction of the DG-TREN (2006b) was to format a new proposal that combines the following criteria:

1. Ports in which the Directive 65/2005 is applicable;
2. Ports in which the Regulation 725/2004 is applicable;
3. Ports that are part of the TEN-T, according to the Decision 1346/2001;
4. The type and volume of the cargoes handled in a port and the presence of alternatives:
 - a. Ports that handle vessels from/to EU member states,
 - b. Ports that handle cargo volume above a threshold,
 - c. Ports that handle dangerous types of cargo (e.g. LNG),
 - d. Ports where no suitable neighbouring alternative port exists.

Using these variables DG-TREN suggests that those ports that fulfil the three first criteria as well as the combination 4.a+4.b+4.d, or the combination 4.a+4.c+4.d, should be characterised as European Critical Infrastructures.

To overcome the situation, the Commission has put forward a proposal for a directive that establishes a procedure for the identification and designation of European Critical Infrastructures, and a common approach to the assessment of the needs to improve the protection of such infrastructures (CEU, 2006b). Then, a sector-by-sector European project will be deployed for the protection of these infrastructures on the basis of the principles of: subsidiarity; complementarity with existing sectoral measures; confidentiality of information; stakeholder cooperation; and proportionality to the level of risk and type of threat involved (CEU, 2006c).

Given the existing number of sectoral measures, it is not likely that seaports will be addressed in an early phase of the implementation of the directive. This is because. In addition, the proposal for the aforementioned directive as it stands, explicitly exempts seaports from the requirement to establish such a plan. This is because it is acknowledged that Directive 2005/65 on enhancing port security already satisfies the requirement to establish an Operator Security Plan. Moreover the Commission indicated that, although not entirely identical, the Port Security Officer existing under the Directive 2005/65 serves as a basis for the designation of a SLO. In the same vein, stakeholders and member states in the field of transport have already agreed on the absence of

⁸ The other ten identified sectors are: energy, nuclear industry, information and communication technologies, water, food, health, financial, chemical industry, space, and research facilities.

an immediate need to impose additional security measures on ports, which are nevertheless already covered by the Directive on port security.

Beyond all these rules, the third maritime safety package (CEU, 2005b). During the discussions of the proposed Directive, the Council of Ministers (2005) included in its Annex VII procedures that Port State Control authorities must follow for inspecting and controlling ships compliance with security related rules. If transposed to an EU rule, these procedures will give the authority exercising Port State Control, the right of inspection of the security conditions onboard the ship and if required, the detention of the ship.

4.6 EU Security: A Holistic Approach

Along with Regulation 2320/2002 that the EU has adopted in order to address security issues of air transport⁹, the preceded efforts of the EU on safeguarding the transport chain from unlawful acts have resulted, in an extensive regulatory framework, which applies in every part of the transport chain (Figure 1).

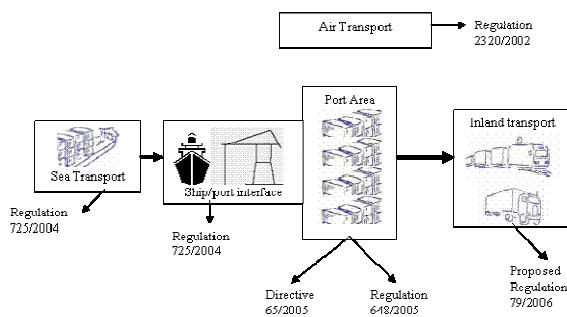


Fig. 1: The European supply chain security regulations

The EU regulations 2320/2002, 725/2004, and 648/2005 are already in force. The same is true as regards Directive 65/2005. Regarding the EPCIP the stakeholders' consultation is in process the stage a Communication is expected to be published within 2007. Relevant legislative initiatives remain an option for the future. Finally, the European Commission is also expect to publish a communication putting forward a proposal for a regulation on enhancing supply chain security.

Geopolitical developments induced a widespread acknowledgment of the need for a major effort to secure the port area and maritime transport in order to prevent unnecessary security incidents. Yet, port authorities have been sceptical about the aforementioned supranational EU policies. Reactions mainly focused on the need to avoid a 'one size fits all ports' approach and on the transfer of the responsibility for inspections to a supranational level. Via the European Seaports Organisation (ESPO, 2004) port authorities expressed the view that the Commission's role should be limited to verifying the overall implementation of the general principles of Directive 65/2005 and Regulation 725/2004 by member-states.

Moreover, port authorities strongly reacted to a potential EPCIP advocating that there is no need for another security regulation in ports, as it would place an unnecessary burden on commercial activities with adverse effects. Their view is that this programme might result in situations that a carrier may choose a port that has been characterised as critical infrastructure, solely because this would suggest that he enjoys increased security.

Also they believe that the proposed regulation on enhancing supply chain security is another unnecessary regulatory burden, as the port sector is already secured by the existing policy regime and asked for an exclusion of ports from any additional measures. ESPO has also stressed the contradiction between the proposed regulation on supply chain security and the ISPS Code. The latter implies stricter inspection measures at the port points of entrance and exit, while the former requests fewer checks for the 'secure operators' at ports. Port authorities are also negative to the introduction of voluntary schemes and favour a mandatory minimum basic security standards regime. This is because in the case of a voluntary scheme, the weaker parts of the supply chain would face difficulties in participating due to their inability to finance the substantial costs involved (ESPO, 2006).

Via, their European federation (FEPORT), European private port operators have questioned the need for developing further security standards, advocating that new measures would impose additional requirements only few months after ISPS implementation. This development would devalue the costly ISPS security systems which have been just put in place in many European ports.

On the contrary, European freight forwarders are in favour of a voluntary supply chain security scheme. Yet, via the European Association for Forwarding, Transport, Logistics and Customs Services (CLECAT) they have requested certain actual incentives for companies that will participate and implement the requirements of this scheme (i.e. partial compensation for their expenses) therefore a major importance is placed on the re-examination of the liability issue (CLECAT, 2006). Specifically, it is of primary interest to associate the status of the 'secure operator' with the opportunity to insure the operation and the eligibility for compensation in the case of a major incident. Freight forwarders advocate the need for an advisory stakeholders' group, similar to the Stakeholders' Advisory Group on Aviation Security (SAGAS). Pointing out that all security regulations and statuses have many common requirements or identical criteria and cause confusion to operators, they suggest that this group could contribute to the simplification of the security processes and the related statuses. The work of the established Stakeholders' Advisory Group on Maritime Security (SAGMAS) is underway.

5. Security Related Costs and Benefits

The benefits of the EU rules addressing supply chain,

⁹ Regulation 2320/2002 establishing common rules in the field of civil aviation security". OJ L. 355, 30.12.2002.

port and ship security are accompanied by substantial implementation costs. The allocation of these costs and the presence of uniform methods of financing this implementation are two controversial issues. In the case of the port sector a number of policy-makers and stakeholders have expressed diverge approaches, mainly because of the presence of organisational, management and port financing dissimilarities.

5.1 Implementing Regulation 725/2004

The costs of the ISPS Code implementation as detailed in Regulation 725/2004 largely depend on the peculiarities of each ship or port, rather than on a standard and uniform approach for every ship or port. The challenge is to address potential ways of financing this implementation. Then, there is the question of how to incorporate these costs into pricing and marketing strategies, when at the same time these ports maintain their market shares and achieve reasonable profit margins (cf. Bichou, 2004). Today, terminal security fees as charged by operators vary significantly, as do the approaches as to financing and recovering schemes.

For a port facility located in the EU the average initial investment cost in order to implement the ISPS in line with Regulation 725/2004 has been estimated at \$464.000. The annual running costs are estimated at \$234.000 (RMG, undated)¹⁰.

There are three distinctive approaches as regards the finance of this implementation (cf. UNCTAD, 2006):

- The facility operators might finance the entire cost which is then recharged to customers;
- The port authority might cover the financial burden;
- The cost might be shared between different parties, with each one assuming responsibility for recovering its own costs.

Identifying the most suitable scheme remains an issue more complex than in cases like shipping (responsibility lies with its operator) due to the various ownership and management structures. According to the Rotterdam Maritime Group (RMG, undated) 19% of port facilities increased port tariffs in order to recover the implied costs and 55% have imposed a separate ISPS tariff. Another 23% have opted to finance the cost of the ISPS implementation from subsidies. Assuming that these subsidies are provided by public entities, the private sector finances the cost in 74% of the total number of port facilities (CEU, 2006d). Most European ports have introduced port container security charges to recover initial expenditures. In 2006 the average terminal security fees were 10,98 \$/TEU in Belgian Ports, 10,37\$/TEU in Dutch ports; 10,98 in French ports; 9,76 in Italian ports; 6,1 in Spanish ports; and 8,54 in Irish ports.¹¹ Yet the presence of public funds in some cases questions the impact on the conditions of competition in the sector.

¹⁰ The same study estimated that the implementation of the ISPS Code for shipping companies demands an average investment of \$98.109 per vessel and an annual running cost of \$25.000 per vessel.

¹¹ Summary of various news articles from Lloyd's List, Fairplay and Containerisation International; as quoted in: UNCTAD, 2006.

The lack of a EU rule regarding state aid creates further ambiguities regarding the impact of security measures on port competition. On the one hand, it is argued that the mobilisation of public funds for implementing security measures contradicts Article 87(1) of the EU Treaty on state aid, as it distorts market conditions. On the other hand, it is advocated that the EU Treaty acknowledges that public finance which is devoted to the implementation of measures imposed by law and connected with the exercise of powers, typically those of a public authority, does not constitute economic activity. Thus, the public financing of transport security measures does not constitute state aid. The potential to overcome this situation and achieve the smooth implementation of the EU security related port measures is inextricably linked with the presence of clear guidelines or regulations, creating a homogenous regime insofar as state aid to European ports and the transparency of their financing are concerned.

Directive 65/2005 results in additional security obligations spreading cost related concerns. ESPO and the Federation of private port operators (FEPORT) endorse the view that security is a public good and should be covered by public funding. The latter should also cover the costs made by the designated authority (the formation of which is required under the directive) and the recurred overhead costs (audit and control). The users of the specific port facilities should cover all other costs.

The major benefit of Regulation 725/2004 and Directive 65/2005 is the elimination of the risk of an unlawful act. The higher the risk - which equals the possibility of an action/element to occur, multiplied by its consequences - the higher the adverse effect on the operators' returns (Carter and Simpkins, 2002), and on the operating companies' capacity to remain attractive to capital investors (Homan, 2006). Security policies do not only reduce the threat from unlawful acts and the direct costs that the latter might produce. They also reduce the systematic risk, which is a primary component of a firm's weighted average cost of capital (Hamada, 1969).

Stricter security measures produce ancillary economic benefits, including invisible collateral benefits, such as the improvements in efficiency and trade facilitation that are difficult to be measured where no security incidents occur (Rice and Spayd, 2005). Temporary closures of a seaport result in highly variable product delivery lead times and thus increase supply chain inventory management costs. Since short port closures typically lead to ships waiting to off-load cargoes, the long-run average cost for a firm operating a supply chain that uses a seaport subject to unexpected closure increases (Lewis *et al*, 2006). Beyond these benefits, the presence of uniform security requirements for all European ports eliminates potential competition distortions and contributes to a level playing field within the Single European Market.

5.2 Implementing the Proposal on Supply Chain Security

The proposed Regulation on enhancing supply chain security has an effect on all the elements integrated in

this chain. The number of enterprises in EU's 25 to be affected, stands to approximately 4,75 million (DNV Consulting, 2005). In the case of the port sector, economic effects (costs) have a reference to the integration of inland transport modes (road, train, inland shipping) and the providers of value-added services and value-added logistics within the port area. There are also additional requirements for port operators such as the fast track treatment of the 'secure operators'. The development of maritime supply chain underlines the interaction between security issues and management strategies of ports around the world (Flemming, 1999).

For the moment, there are three potentials as regards supply chain security. The first one is for the situation to remain as it is. The second is the development of a voluntary scheme. The third option is for a mandatory EU policy, implementing common security rules.

The cost for the implementation of either the potential mandatory or voluntary schemes derives from the demands for inspection of security measures, the audit of the implementation status, the enforcement of the requirements, etc.

In the case of a mandatory scheme, the costs are estimated to range from €5.000 to €300.000 (Table 5.1). Based on an estimated number of companies in each category, the cost of implementation will reach a total of €60 billion for all the companies participating in European supply chains. For member states the costs for verifying implementation through audit will be €3,867 billion: €2,7 billion initial verification, plus €1,167 billion for annual verification thereafter (DNV Consulting, 2005). This corresponds to an auditing cost of €0,55 per EU citizen per year (CEU, 2006e). There is an additional cost of enforcement estimated at €450 million for an initial three-year period plus €50 million per annum thereafter. In practice there are further costs because of the required aftermath actions (such as the awareness campaign, the employee vetting system, and the EU seal programme) resulting in a higher final total cost.

Table 1: Costs for implementing a mandatory Security Management System (DNV Consulting, 2005)

Company type	Employees	Estimated costs for implementing a SMS
Micro companies	1-9	5.000
Small companies	10-49	50.000
Medium companies	50-249	135.000
Large companies	?250	300.000

The endorsement of a voluntary scheme in Europe is estimated to attract approximately a maximum of 904.500 companies, or 75% of all freight flows within 5 years from the introduction of the regulation. In this case, the cost for the supply chain companies will reach €12,1 billion. The enforcement cost will remain €450 million for the first three-year period but there will be

no annual enforcement cost thereafter. Finally, the auditing cost will be substantially lower and estimated at €514 million for the initial verification and €227 million for the annual auditing cost (DNV Consulting, 2005).

As Table 2 summarises, a mandatory scheme requires significantly higher funds than the voluntary scheme. There are further questions regarding the potential of a mandatory scheme. Many companies, especially the small ones that are the vast majority of the companies participating in the supply chain, place hardly any importance on security. Proper implementation will be difficult to succeed as these companies cannot afford it. Moreover, these are mostly companies of national importance which do not think that security measures will give a competitive advantage to their operations. Taking into account all these, it seems probable that the EU institutions might finally endorse the, advocated by the Commission, voluntary scheme.

Table 2: Mandatory and voluntary schemes major costs: A Comparison (DNV Consulting, 2005)

Cost	Mandatory	Voluntary
Supply chain companies	€60 billion	€2,1 billion
Member States (audit, implementation)	€2,7 billion initial three years period + €1,167 billion p.a.	€514 million initial three years period + €227 million p.a.
Enforcement	€450 million + €50 million p.a.	€450 million
Coverage (freight flows)	100% (4,75 million companies)	75% (904,500 companies)

The benefits of the endorsement of any of the two schemes extend the societal benefits resulting from trade facilitation, the reduction of the risks of human casualties and economic damage from a security incident, and the increased confidence in the supply chain. For the participating companies there are further benefits resulting mainly due to the reduction of cargo theft, the prevention of damage to the brand, and the reputation of a company. A cargo theft reduction by 10% will result in €10 billion savings for the EU economy (DNV Consulting, 2005). The short-term effects might be negative due to the required investments, but the medium to long-term impacts are likely to be beneficial, at least for the certified and recognised operators (Bano-myong, 2005).

An additional issue that remains to be addressed is the fair distribution of the costs of the new rules. In the absence of a common approach in all security related policies the funding regime might distort competition. The Directive on port security emphasises that the financing of security measures has to be shared between public authorities, port authorities and operators. On the other hand, the proposed EPCIP recommends that the owner/operator of the European critical infrastructure should finance the preparation of the operator security plan and the work for Security Liaison Officer.

Recently, the Transport Committee of the European Parliament backed a report asking the national governments to share the costs of security measures in airports (Euractiv, 2007). This approach and the relevant contra-

dictive proposals show the lack of a uniform framework for financing security. With substantial financial obligations in fulfilling security requirements, the issue would like to further complicate existing questions on the EU agenda regarding who should fund such port security measures, as well as whether the provision of state-aids should continue for the sake of higher security. Different countries maintain different policies and perceptions on port operations, management and finance.

An issue that contributes to the 'financing security' question is the fact that the problem of asymmetric information is particularly pronounced regarding security. As Brooks and Button (2005) emphasise, the reaction of authorities in unlawful acts is not exclusively designed to stop the physical damage that unlawful acts might cause. Much of it is aimed at reassuring the public and containing the psychological damage associated with fear. In this sense, a large part of security can, therefore, be seen as a public good from which it is difficult to exclude individuals and which is not diminished as more come under the umbrella of public confidence.

Taking into account the increased number of stakeholders in ports and their complex relations (Notteboom and Winkelmanns, 2002), as well as the multiplicity of ports' ownership, operational and management status (Bichou and Gray, 2005), a means to specify the distribution of optimum security costs (financing of an action) is to identify and quantify the benefits that the security measures result in, and then apply the principle "beneficiary pays" (cf. Pallis and Vaggelas, 2005). Nonetheless, the implementation of this efficient (as it includes the distortion of competition) financing of security regulation needs to also take into consideration equity objectives, i.e. the contributive capacity of the different actors involved (Dubecco and Laporte, 2004).

6. Conclusions

Transport security awareness has increased due to recent unlawful acts. In the field of maritime transport, security has moved up on the political agenda worldwide. In this context, the EU has been active legislating in order to improve security at ports, at sea and finally in the whole supply chain. Regulation 725/2004 and Directive 65/2005 stand as the major related regulatory initiatives. The proposed Regulation on enhancing supply chain security, and the European Programme for Critical Infrastructure, which are currently under consideration, are part of the process of incorporating modal rules into an integrated approach of security issues.

The EU measures transformed within a short time a port market that was previous unregulated as regards security issues. The benefits of the secure operation are associated with issues of financing and cost-recovery of the expenditures involved in implementing security measures.

Complaints about an over regulated market and about confusing contradictory requirements by these regulations are not rare. There is also an ongoing debate between the EU institutions and various the port stake-

holders regarding the implementation of 'minimum standards' for security measures. The existing regulations do not specify specific standards to be maintained. The EU institutions are in favour of new measures detailing such standards, while several stakeholders (e.g. ESPO, FEPORT) disagree, believe that the minimum standards would devalue the existing security related regulations while increasing the costs of implementing these regulations. Moreover port authorities, via ESPO, argue that the basis for drawing any new security measures should be the risk assessment of specific activities, rather than an approach based on predefined standards. This is an ongoing still inconclusive discussion.

Nonetheless, it is noteworthy that the enactment of security related EU policies have side-effects as well. As Ng (2007) suggests, while the EU often highlights the necessity of promoting secondary ports to boost the competitiveness of shortsea shipping, ironically, the introduction of port security measures poses the risk of further strengthening the competitive positions of the big ports, especially for feeder traffic. As Ng analyses, many security instruments would inevitably imply the need for considerable financial inputs by ports (in terms of both technological development and personnel training) and it is highly doubtful whether lesser ports in Europe, of which many of them are located within the less developed regions and rely on local limited hinterlands for survival, would possess the financial strength to fulfil such requirements.

The enactment of the EU rules will soon provide a comprehensive security policy addressing all (trans)port issues in an integrating way. The coordination and optimisation within the EC in providing a constructive solution in inscribing security issue in ports, while not affecting the competitiveness, is the way forward. Assuming that the right allocation of economic costs succeeds, the positive effects are apparent. The focus will then be on their proper implementation via the inspection and auditing of the participating member states, port and other relevant authorities, and companies involved in (maritime) transport operations. Finally as in other fields of maritime transport (i.e. safety – cf. Pallis, 2006), the initiative of the EU institutions had to acknowledge that any relevant threat needs a global response, and security measures can be locally defined only in exceptional cases.

References

- Banomyong, R., (2005). "The impact of port and trade security initiatives on maritime supply-chain management". *Maritime Policy and Management*, 32, 1, 3-13.
- Barton, H., and Turnbull, P., (2002). "Labour regulation and competitive performance in the port transport industry: The changing fortunes of three major European seaports". *European Journal of Industrial Relations*, 8, 2, 133 – 156.
- Bichou, K., (2004). "The ISPS Code and the cost of port compliance: An initial logistics and supply chain framework for port security assessment and management". *Policy Perspective, Maritime Economics and Logistics*, 6, 322-348.

- Bichou, K., and Gray, R., (2005). "A critical review of conventional terminology for classifying seaports". *Transportation Research part A*, 39, 75-92.
- Brooks M.R. and Button K. (2005). "Market Structures and Shipping Security. Proceedings of the International Association of Maritime Economists (IAME) 2005 Conference, June 2005, Limassol, Cyprus.
- Carter, D., and Simpkins, B., (2002). "Do markets react rationally? The effects of the September 11th tragedy on airline stock returns". Stillwater: Oklahoma State University.
- CBP (Customs and Border Protection US), (2006a). "Fact sheet". September 2006, Washington DC.
- CBP, (2006b). "Container Security Initiative. 2006-2011 strategic plan". CBP Publication 0000-0703. August 2006, Washington DC.
- CEU (1997). "Green Paper on sea ports and maritime infrastructure". Com (97)678 final, Brussels, 10.12.1997.
- CEU (2001). "White Paper-European transport policy for 2010: time to decide". Com (2001)370 final. Brussels, 12.9.2001.
- CEU (2004a). "Customs: EU and US adopt measures to strengthen maritime container security". IP/04/1360. Brussels, 15.11.2004.
- CEU, (2005a). "Green Paper on a European Programme for Critical Infrastructure Protection". Com (2005)576 final. Brussels, 17.11.2005.
- CEU (2005b). "Proposal for a Directive on Port State Control" (Recast). Com (2005)588 final. Brussels, 23.11.2005.
- CEU (2006a). "Proposal for a regulation of the European Parliament and of the Council on enhancing supply chain security". Com (2006)79 final. Brussels, 27.2.2006.
- CEU (2006b). Proposal for a Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. Com (2006)787, final. Brussels, 12.12.2006.
- CEU (2006c). Communication from the Commission on a European Programme for Critical Infrastructure Protection. Com (2006)786, final. Brussels, 12.12.2006
- CEU (2006d). "Report from the Commission to the Council and the European Parliament on transport security and its financing". Com (2006)431 final. Brussels, 1.8.2006..
- CEU (2006e) Annex to the Communication on enhancing supply chain security and Proposal for a Regulation on enhancing supply chain security- Impact Assessment. SEC(2006)251, Commission Staff Working Document. Brussels, 27.2.2006.
- Chlomoudis C.I. and Pallis A.A. (2002). *European Port Policy: The movement towards a Long-term Strategy*. Cheltenham: Edward Elgar.
- CLECAT, (2006). "Discussion paper".. Brussels: CLECAT, 6.8.2006.
- Council of Ministers (2005). "Third Maritime Safety Package: Proposal for a Directive on Port State Control". W.Doc 2005/67.. Brussels: General Secretariat of the Council, 30 11.2005.
- DG-TREN (2006a). "Minutes of the Expert Group meeting on Critical Maritime Infrastructure". March 28th. Brussels: CEU.
- DG-TREN (2006b). "Element of background". TREN.J.3/RGG/mcgD (2006)213863. 29 June. Brussels: CEU.
- DNV Consulting (2005). "Study on the impacts of possible European legislation to improve transport security". Final report: impact assessment. Report for European Commission, DG TREN. Report No 4000 8032-6-2. Rev 2: final.
- Dubecco, P., and Laporte, B., (2004). "Securing International Trade from Terrorism: The Financing Issue". WIDER Conference on Making Peace Work, June 2004, Helsinki, Finland.
- Euractiv, (2007). "Parliament and Council head for clash on air security costs". www.euroactiv.com, assessed 12 April 2007.
- ESPO (2004). "Response of ESPO to the draft report of the directive proposal on enhancing port security-COM (2004)76".. Brussels, 22.11.2004.
- ESPO (2006) Green Paper on Critical Infrastructure: ESPO's initial views. Available at www.espo.be, assessed December 2006.
- Flemming, D., K., (1999). "A geographical perspective of the transshipment function". Paper presented at the International Association of Maritime Economists (IAME) 1999 Conference, September 1999, Halifax, Canada.
- Hamada, R., (1969). "Portfolio analysis, market equilibrium and corporation finance". *Journal of Finance*, 24, 13-31.
- Henstra, D., Woxenius, J., (1999). "Intermodal transport in Europe". TRILOG report for the European Commission, 99NL/379.
- Homan, A., (2006). "The impact of 9/11 on financial risk, volatility and returns of marine firms". *Maritime Economics and Logistics*, 8, 4, 387-401.
- ILO, (2003). "Seafarer's Identity Documents Convention (Revised)" No 185. Geneva: ILO.
- IMO – ILO, (2003). "Code of practice on security in ports". Tripartite meeting of experts on security, safety and health in ports. Geneva.
- ISO, (2004). "Ships and marine technology-maritime port facility security assessments and security plan development". ISO/PAS 20858. First edition, 2004-07-01, Geneva.
- ISO, (2005). "ISO/PAS 28000. Specification for security management systems for the supply chain". First edition 15-11-2005. Geneva, Switzerland.
- ISO (2006). "ISO/PAS 28001-Specification on best practices for implementing supply chain security, assessment and plans". Publicly Available Specification. March 2006, Geneva.
- Johnston, V., R., (2004). "Transportation security and terrorism: Resetting the model and equations-epilogue". *Review of Policy Research*, 21, 379-402.
- Juhel, M.C., (1998). "Globalisation, privatization and restructuring of ports". 10th Australasian Summit "Ports, Shipping and Waterfront Reform". December 1998.
- Lewis, B.M., Erera, A.L, White, III, C.C., (2006). "Impact of Temporary Seaport Closures on Freight Supply Chain Costs". *Transportation Research Record: Journal of the Transportation Research Board*, No 1963, 64-70.
- Ng A.K.Y. (2007). "Port Security and the Competitiveness of Short Sea Shipping in Europe: Implications and Challenges". In: Bell M., Bichou K., and Evans A. (Eds). *Port and Supply Chain Security in the post 9/11 era: Framework, Models and Applications*, London: Lloyd's of London Press, forthcoming.
- Notteboom, T.E., Rodrigue, J.P., (2005). "Port regionalization: Towards a new phase in port development". *Maritime Policy and Management*, 32, 3, 297-313.
- Notteboom, T.E., Winkelmans, W., (2002). "Stakeholders relations management in ports: Dealing with the interplay of forces among stakeholders in a changing competitive environment". *International Association of Maritime Economists (IAME) 2002 Conference*, Panama, December 2002.
- Pallis A.A., (2002). *The Common EU Maritime Transport Policy: Policy Europeanisation in the 1990s*, Aldershot: Ashgate.
- Pallis A.A., (2006). "Institutional dynamism in the EU Policy-making: The evolution of the EU Maritime Safety Policy". *Journal of European Integration*, 28, 2, 137-157.

- Pallis A.A., (2007). "EU Port Policy Developments: Implications for Port Governance". In: Brooks M.R. and Cullinane K. (Eds.), *Devolution, Port Governance and Performance*, London: Elsevier, 161-176.
- Pallis, A.A., and Vaggelas, G.K., (2005). "Methods for measuring public and private benefits from port services provision: A comparative study". International Association of Maritime Economists (IAME) 2005 Conference. Limassol, Cyprus, June 2005.
- Psaraftis H.N. (2005). "EU Ports Policy: Where do we Go from Here?". *Policy Perspectives, Maritime Economics and Logistics*, 7,1, 73-82.
- Power, V. (1992). *The EC Shipping Law*. London: Lloyd's of London Press.
- Rice, J.B.Jr., and Spayd, P.W., (2005). "Investing in supply chain security : Collateral benefits". Cambridge, US: Massachusetts Institute of Technology.
- Robinson, R., (2002). "Ports as elements in values-driven chain systems: The new paradigm". *Maritime Policy and Management*, 29, 3, 241-255.
- Rotterdam Maritime Group (RMG) (undated). "Study on maritime security financing -Final report". TREN/05/ST/S07.48700. In cooperation with the Swedish Maritime Administration, Rotterdam: RMG.
- Slack, B., (1998). "Intermodal Transportation". In: Hoyle, B.J., Knowles, R.D. (eds.) *Modern transport geography*. Second ed. Chichester: Wiley, 263-289.
- UNCTAD, (2004). "Container Security: Major initiatives and related international developments". Report by the UNCTAD Secretariat: February 2004, New York and Geneva: UN.
- UNCTAD, (2006). "Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment". UNCTAD/SDTE/TLB/2005/4. New York and Geneva: UN.
- World Customs Co-Operation Council (WCO), (2004). "Resolution of the customs co-operation council on global security and facilitation measures concerning the international trade supply chain". June, Geneva: WCO.