

# Ship, port and supply chain security concepts interlinking maritime with hinterland transport chains

Gerhard Schilk<sup>1)</sup>, Eberhard Blümel<sup>2)</sup>, Valerio Recagno<sup>3)</sup>, Wando Boevé<sup>4)</sup>

<sup>1)</sup> via donau – Österreichische Wasserstraßen Gesellschaft mbH, Austria, [gerhard.schilk@via-donau.org](mailto:gerhard.schilk@via-donau.org)

<sup>2)</sup> Fraunhofer Institute for Factory Operation and Automation, Germany, [eberhard.bluemel@iff.fraunhofer.de](mailto:eberhard.bluemel@iff.fraunhofer.de)

<sup>3)</sup> D'Appolonia S.p.A, Italy, [valerio.recagno@dappolonia.it](mailto:valerio.recagno@dappolonia.it)

<sup>4)</sup> European Intermodal Research Advisory Council (EIRAC), Belgium, [Secretariat@Eirac.net](mailto:Secretariat@Eirac.net)

## Abstract

*As maritime processes do not stop at sea ports, hinterland operations have to be considered and addressed as well. This becomes obviously on designing and managing seamless cargo and information flows from/to hinterland regions via sea ports from/to transcontinental markets. Nowadays, also security-related aspects need to be tackled in order to enable continuous flows corresponding to security legislations and technical requirements set up in the field of maritime and intermodal hinterland transport. Ensuring transport security within the European transport market requires both adequate security legislations and innovative concepts. While for the maritime sector, including sea ports, security regulations are already in force, hinterland operations (road, rail and Inland Waterway Transport) are only indirectly affected today, either on carrying out transports from/to sea ports or exporting commodities to overseas territories. This results in the need for innovative security strategies and concepts combining maritime with hinterland transport enabling seamless security processes.*

## Keywords

Maritime; hinterland; intermodality; security in transport-logistics; EIRAC

## 1. Introduction

### 1.1 Transport and logistics in Europe

The European Commission (2001) stated the growth of goods transport within the EU, at a rate of 2.8% per year, was broadly in line with economic growth, which was 2.3% on average in the period 1995-2004. Overall, goods transport grew by 28% and passenger transport by 18% during the period 1995-2004, with transport by road growing by 35% and 17% respectively. Short sea shipping grew at almost the same rate. Rail freight transport in those Member States that have opened up

the rail market early showed a bigger increase compared to the other countries. Overall, rail freight transport grew by 6% in 1995-2004. Intra-EU air travel grew by more than 50% in the same period despite the decline following the 11 September attacks, integrating the effects of the liberalisation that had already begun in the late 1980s. Inland waterways transport showed strong growth in the last decade in certain Member States (i.e. 50% in Belgium, 30% in France).

Additionally it declared that the largest share of intra-EU transport is carried by road, which accounts for 44% of freight and around 85% of passenger transport. Demand factors, such as a reduction in heavy bulk transport and the increasing importance of door-to-door and just-in-time service, undoubtedly contributed to the strong sustained growth of road transport. Among the main structural trends is the fact that rail freight transport has halted its relative decline since 2001 and is on a growth path in a number of Member States. Another salient trend is the strong and sustained dynamism of air and waterborne transport. Maritime transport accounts for 39% of internal goods transport and nearly 90% of the external trade volume. One quarter of ships in the world fly a European flag; 40% are European-owned.

As major waterways exist only in certain Member States of the European Union (EU), inland waterway transport accounts for only 3% of overall goods transport; this mode of transport still harbours considerable unexploited potential. Whereas the 2001 White Paper assumed an average economic growth rate of 3%, the actual outcome in the period 2000-2005 was 1.8%. For the period between 2000 and 2020, forecasts establish the average annual GDP growth rate at 2.1% (52% for the whole period). Freight transport is expected to grow at roughly similar rates (50% for the whole period) whereas passenger transport growth is expected to be lower at the order of 1.5% on average annually (35% over the whole period).

### 1.2 Transport Security

#### (1) Security

Safety and security are not the same! While safety addresses all activities dealing with safe processes (transport, transshipment, storage etc.) with special focus on accidents which might happen hereby, security has a different origin. Security comprises all activities related to intentional unlawful acts, such as property violation, robbery, fraud, stowaways, contraband, vandalism, and since 2001 terrorism as well. Therefore, security will become a more complex topic in Europe by covering on several security issues; besides terrorism and related common crime (e.g. theft, fraud).

**Table 1: Security versus safety**

Terms	Origins	Examples
Safety	Accidents	Road accidents, damages etc.
Security	Incidents	Common crime (e.g. property violation) <b>and</b> terrorism

The European Commission (2003) informed that the direct costs of breaches in transport security, particularly theft, cost the European economy several billion of euros each year. The costs of a major terrorist incident (e.g. interruption of trade, loss of life, cost of diversions etc.) involving a key piece of transport infrastructure could be of major concern for the European economy.

Moreover it declared that crime and terrorism are not limited by national boundaries, nor are they focussed on a single transport mode. In order to protect the whole transport chain, it is necessary to ensure that all transport service providers operate to agreed standards. To avoid distortions of competition, to guarantee the integrity of the Union's external frontier and to ensure the functioning of the single market, security standards must apply across all modes of transport: waterborne, road, rail and aviation. Of course, measures may vary according to the specific risk that each transport operation, equipment or infrastructure is exposed to. The final purpose of these security measures is to protect the European transport system (vehicles, infrastructure, employees, passenger and cargo) from intentional unlawful acts. In fact, the security performance of a transport chain is as strong as the weakest element along the chain.

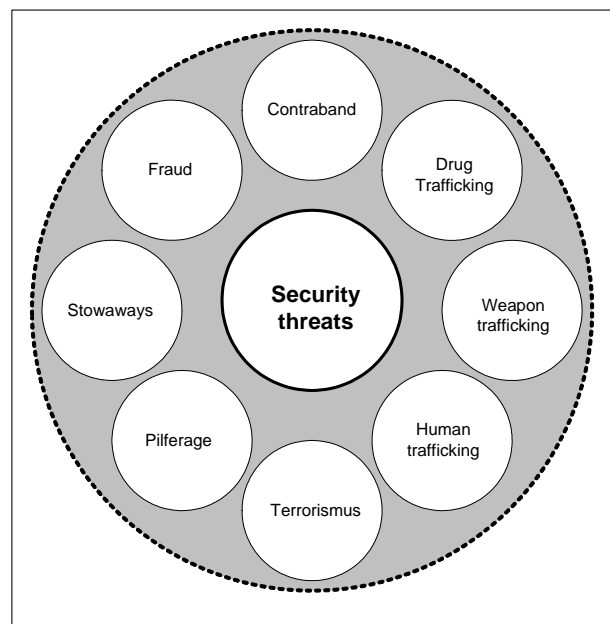
(2) Transport Security

Security in the European transportation sector has been improved significantly. A European security framework has been created for civil aviation and maritime as well as port security has been intensified, endorsing the prescription produced by international standardisation bodies. Maritime and air transport companies are active in spatially bounded, clearly defined and controllable areas. Security measures are nothing unusual for them. Surface transport in its entirety has completely different dimensions. Over half a million companies, ranging from large multinationals to small service providers, are active in the transportation sector alone. They are rooted

in an array of cultures and business environments. Few have any security management or have only now begun to implement appropriate measures.

The European Commission (2003) proposed that transport security is the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems and workers against intentional unlawful acts.

- Transport infrastructures should be protected against terrorism and other intentional unlawful acts.
- The theft of goods in transit is a major problem for European industry which is costing billions of euros a year. These thefts are not only a burden on industry (replacement costs, lost sales, customer dissatisfaction) but also the proceeds from these crimes may be used to fund other criminal activity.
- Criminals might attempt to introduce drug, weapons or explosives into a legitimate shipment on route, or may even transport illegal products disguised as a legitimate shipment. This requires improvements to the security of shipments.
- Criminals might attempt hijack vehicles often to steal cargo but also potentially to use it as a weapon. This requires improved preventive measures and mitigation strategies (e.g. locks).
- Measures should hence protect infrastructure, prevent or reduce the impact of security incidents and ensure a coherent set of measures are applied across modes and countries to prevent breaches of security or distortions of competition.



**Fig. 1: Selected list of security threats in transport processes and operations**

An analysis of the supply chain reveals that it is divisible into four spheres of activity each with its own security requirements:

1. Preparation and shipment of goods at their place of manufacture,
2. Transport of goods,
3. Freight forwarding,
4. Operation of handling and storage facilities as well as inland terminals.

Complex information processes are part of every link in transport, logistics and supply chains.

Security of operations: The handling of incoming and outgoing goods should involve security operations that prevent material from being brought in, exchanged or removed:

- Monitoring the delivery/removal of cargo,
- Properly labeling, weighing, payment and documentation of cargo,
- Inspecting the intactness of seals or other security features of incoming cargo,
- Sealing or otherwise protecting outgoing cargo,
- Identifying and reporting missing or surplus cargo,
- Tracking incoming and outgoing goods,
- Appropriately storing empty and full loading units to prevent unauthorized access etc.

## 2. Security issues in maritime and hinterland processes

Innovative security concepts are needed for interlinking efficiently maritime with hinterland transport chains including maritime ships, sea ports and intermodal hinterland transport comprising road, rail and Inland Waterway Transport (IWT).

- Firstly, ship and port security need to be addressed, as security legislations for this specific mode of transport are already in place since several years; this both at international level (the ISPS-Code), in the United States (e.g. Container Security Initiative, 24h-manifest, C-TPAT), and in the European Union (e.g. 725/2004, 65/2005). It was well understood that port security has to be focussed as sea ports are the gateway from/to hinterland territories and supply vital cargo flows to the customers.
- Secondly, hinterland transport including all (intermodal respectively multimodal) transport and logistics processes from/to sea ports forms the most essential interface between maritime and land-surface transport modes like road, rail and Inland Waterway Transport (IWT). Until today, for this section of transport flows there is no security legislation in place. However, some security initiatives (e.g. 79/2006, 787/2006) are currently under preparation. Besides these initiatives, one has to bear in mind that also the prevailing US/EU-security legislations, which have been issued for other specific modes (e.g. maritime security), have indirect effects on hinterland processes.

### 2.1 Ship and port security

Following, freight transport security affairs with respect to ship and port security will be described and analysed.

#### (1) Security threats in maritime transport and sea ports

OECD (2003) declared that perhaps foremost among the risk factors associated with maritime transport is the sheer volume and numbers of goods transported by sea. The United Nations Conference on Trade and Development (UNCTAD) estimates that 5.8 billion tons of goods were traded by sea in 2001. This accounts for over 80% of world trade through the world. In addition to its size, the maritime sector, by its nature as a complex, international open transport network, poses several additional challenges from security standpoint. One of these is the multiplicity of terrorist risk factors associated with shipping. Moreover it declared that sea-going vessels can be the vector for, or target of, attacks. They can also serve to facilitate other attacks and/or raise revenues for terrorist organizations. The principal risk factors related to shipping – cargo, vessels, people and financing – are also linked to broader risk of major disruptions in world trade and increased economic costs linked to heightened security.

Rand (2003) discovered that approximately 90% of all cargo moves in containers. Approximately 250 million containers are shipped annually. This massive flow of containers around the world is the driving force of the world's economy. Thus, the global shipping system is a critical infrastructure for the global economy, it is, however, also very vulnerable. Estimates are that the contents of less than 2% of all containers are checked to verify that what is inside these containers is actually what is said to be inside the containers. In fact, containers are used by criminals to transport all sorts of banned goods, even people. The problem of the illegal transport of goods and people takes on particularly worrying proportions in light of recent terrorist activities. Terrorists could, use containers to transport dangerous materials, weapons, or use the containers themselves as weapons of mass destruction. The potential threat of terrorists using containers poses a large risk to our economies and to our societies.

Seaport security receives substantial focus because seaports have been widely regarded as vulnerable to attack. One reason is that the nation's seaports play a vital role in the nation's economy and national security. A second reason that seaports are potentially vulnerable is the wide range of targets and attack possibilities they encompass. Facilities such as container terminals, where containers are transferred between ships and railroad cars or trucks, must be able to screen vehicles entering the facility and routinely check cargo. Chemical factories and other installations where hazardous materials are present must be able to control access to areas containing dangerous goods or hazardous substances. Vessels, ranging from oil tankers and freighters to tugboats and passenger ferries or cruise ships, must be able to

restrict access to onboard areas, such as the bridge or other control stations critical to the vessels' operation. Possible terrorist scenarios range from the use of improvised explosive devices to attack ferries to the use of recreational boats to ram key infrastructure in and around ports, according to the United States Government Accountability Office (2005).

## (2) Legislation

After the terrorist attacks starting in 2001, attention shifted from aviation to maritime security, as it became evident that this mode of transport guarantees by most extent global transport and trade. As a consequence international organisations, such as International Maritime Organisation (IMO), and US-administrations started with legislative frameworks addressing maritime traffic and transport operations affecting not only US territories, but also indirectly actors in the European transport and logistics sector. In 2004 the European Commission prepared individual security legislations, which rely primarily on existing ones published on international level before.

- Container Service Security (CSI)
- 24-Hour Advance Vessel Manifest Rule
- Custom-Trade Partnership Against Terrorism (C-TPAT)
- Coast Guard and Maritime Transportation Act (MTSA)
- ISPS-Code (IMO)
- EC-Regulation 725/2004
- Directive 2005/65/EC

### (a) Container Security Initiative (CSI)

In the aftermath of the terrorist attacks on September 11, 2001, U.S. Customs Service, now U.S. Customs and Border Protection (CBP), began developing antiterrorism programs to help secure the United States. Within months of these attacks, U.S. Customs Service created the Container Security Initiative (CSI). The primary purpose of CSI is to protect the global trading system and the trade lanes between CSI ports and the U.S. Under the CSI program, a team of officers is deployed to work with host nation counterparts to target all containers that pose a potential threat. Announced in January 2002, CSI was first implemented in the ports shipping the greatest volume of containers to the United States. In addition to the current 42 foreign ports (Feb. 2006) participating in CSI, many more ports are in the planning stages. By the end of 2006, the number is expected to grow to 50 ports, covering 90% of transpacific maritime containerized cargo shipped to the U.S. CSI is now operational in ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America declared Global Security (2006).

DHS (2006) informs that CSI addresses the threat to border security and global trade that is posed by potential terrorist use of a maritime container to deliver a

weapon. CSI uses a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. Through CSI, the Customs and Border Protection (CBP) officials work with host customs administrations to establish security criteria for identifying high-risk containers. Those administrations use non-intrusive inspection (NII) and radiation detection technology to screen high-risk containers before they are shipped to U.S. ports. DHS (2006) says also that CSI is a deterrent to terrorist organizations that may seek to target any foreign port. This initiative provides a significant measure of security for the participating port as well as the United States. CSI also provides better security for the global trading system as a whole. If terrorists were to carry out an attack on a seaport using a cargo container, the maritime trading system would likely grind to a halt until seaport security is improved. Those seaports participating in the CSI handle containerized cargo far sooner than other ports that haven't taken steps to enhance security.

### (b) 24-Hour Advance Vessel Manifest Rule

U.S. Customs Service has implemented a new Advance Manifest Rule, effective December 2, 2002, that required significant changes to the shipment processes for all cargo on vessels that call on the United States. This had an impact on many of our customers, as it requires that both shippers and carriers adopt new disciplines and processes to ensure timely manifesting and loading of cargo. The Customs Regulations requires all ocean carriers or non-vessel operating common carrier (NVOCC) to submit accurate presentation of certain manifest to US Customs at least 24 hours prior to lading at the foreign port if that vessel is calling a US port direct. Furthermore, the US will advance the chances of detecting terrorist activity as well as assisting its trading partners by using IRS, intelligence reports and other data at their disposal to cross-check company and individual identities. The rule became effective on 2 December 2002 and fully enforced as of 2 February 2003 informs Maersk Logistics (2006).

### (c) Custom-Trade Partnership Against Terrorism (C-TPAT)

In direct response to 9/11, the U.S. Customs Service, now U.S. Customs and Border Protection (CBP) challenged the trade community to partner with CBP to design a new approach to supply chain security focused on protecting the United States against acts of terrorism by improving security while simultaneously speeding the flow of compliant cargo and conveyances. The result was the Customs-Trade Partnership Against Terrorism (C-TPAT) – an innovative, voluntary government/private sector partnership program. C-TPAT builds on the best practices of CBP/industry partnerships to strengthen supply chain security, encourage cooperative relationships and to better concentrate CBP resources on areas of greatest risk. It is a dynamic, flexible program designed to keep pace with the evolving nature of the

terrorist threat and the changes in the international trade industry, thus ensuring the program's continued viability, effectiveness and relevance. Flexibility and customization are important characteristics of C-TPAT. This partnership between CBP and the trade is built on Customs border authority and cooperative relationships. It is built on knowledge – that the trade partner has demonstrated a commitment to supply chain security, and trust – that the company will continue to do so with minimal CBP examination. To uphold this relationship, accountability is required. The trade partner must be willing to assume responsibility for keeping his supply chain secure to agreed upon security standards through self policing and implementing changes as needs arise according to US Customs & Border protection (2007).

(d) Coast Guard and Maritime Transportation Act (MTSA)

The Coast Guard and Maritime Transportation Act covers all maritime transport security affairs related to US maritime traffic and transport operations, according to US authorities (2004): (Selected examples)

- Maritime information
- Maritime transportation security grants
- Joint operational centers for port security
- Vessel and intermodal security reports

(e) ISPS-Code

The International Ship and Port Facility Security Code (ISPS Code) is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. The ISPS Code is implemented through chapter XI-2 Special measures to enhance maritime security in the International Convention for the Safety of Life at Sea (SOLAS). The Code has two parts, one describing mandatory requirements, and one set in form of guidelines. In essence, the Code takes the approach that ensuring the security of ships and port facilities is a risk management activity and that, to determine what security measures are appropriate, an assessment of the risks must be made in each particular case. The purpose of the Code is to provide a standardised, consistent framework for evaluating risk, enabling Governments to offset changes in threat with changes in vulnerability for ships and port facilities through determination of appropriate security levels and corresponding security measures, according to IMO (2007).

(f) EC-Regulation 725/2004 on enhancing ship and port facility security

The European Commission (2004) declares that main objective of this Regulation is to introduce and implement Community measures aimed at enhancing the security of ships used in international trade and domestic shipping and associated port facilities in the face of threats of intentional unlawful acts. The Regulation is

also intended to provide a basis for the harmonised interpretation and implementation and Community monitoring of the special measures to enhance maritime security adopted by the Diplomatic Conference of the IMO on 12 December 2002, which amended the 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) and established the International Ship and Port Facility Security Code (ISPS Code).

(g) Directive 2005/65/EC of 26 October 2005 on enhancing port security

The European Commission (2005) declared on 31 March 2004 the European Parliament and the Council of the European Union adopted Regulation (EC) No 725/2004 on enhancing ship and port facility security. The maritime security measures imposed by that Regulation constitute only part of the measures necessary to achieve an adequate level of security throughout maritime-linked transport chains. That Regulation is limited in scope to security measures on board vessels and the immediate ship/port interface. This means that the main objective of this Directive is to introduce Community measures to enhance port security in the face of threats of security incidents. This Directive shall also ensure that security measures taken pursuant to Regulation (EC) No 725/2004 benefit from enhanced port security. The measures laid down in this Directive shall apply to every port located in the territory of a Member State in which one or more port facilities covered by an approved port facility security plan pursuant to Regulation (EC) No 725/2004 is or are situated. And, it shall not apply to military installations in ports.

(3) Effects on maritime traffic

The OECD (2003) declares that the fear that terrorists could exploit the container transport system for their ends was confirmed on 18 October 2001 when port authorities in the southern Italian port of Gioia Tauro (Italy) discovered a stowaway within a well-appointed shipping container complete with bed, heater, toilet facilities and water. The man's belongings included a cell phone, a satellite phone, a lap-top computer and, ominously, given recent events, airport security passes and an airline mechanic's certificate valid for New York's JFK, Newark, L.A. International and O'Hare airports in the United States. After his arraignment and subsequent release under bond, the stowaway disappeared before further information could be gathered.

Besides the described security threat 'stowaways', of course, all other prevailing types of security threats can have impacts on maritime traffic and sea ports operations. This includes also piracy. Hereby, the OECD (2003) discloses that in 1999 285 vessels have been officially attacked worldwide, while in the year 2000 already 469 have been the target of pirates' activities.

An important risk factor in maritime transport is not only the maritime traffic on open sea itself, but also sea ports, which form a gateway for all imports and exports

from/to a dedicated country or even region. Coordinated attacks at sea ports could have tremendous short- and medium-term impacts on the economy. Likewise attacks on other major ports such as Hong Kong, Singapore, Rotterdam or Antwerp could have devastating impacts on both the regional and global economy, according to the OECD (2003).

## 2.2 Hinterland security

Following, freight transport security affairs with respect to hinterland security will be described and analysed.

### (1) Security threats in hinterland transport supply chains

The level of security has to be defined based on the type of cargo being transported, the position of a company in the supply chain and the vulnerability of the infrastructure. Security measures equally pertaining to all companies would disrupt the supply chain. Companies are increasingly defining their own security standards to protect their own activities and brands and to support their selection of partners. Hence, one single comprehensive action to enact regulations and measures for the supply chain similar to air and maritime transport is impossible in practice. Defining minimum security requirements that can be progressively adapted to technical advances and emerging risks is a more realistic approach to providing adequate security in a given field of operations. Supply chains include a multitude of transport operations and supporting processes between the place of a good's manufacture and its destination. These operations are interrelated just like the companies that execute them. In order to attain a high level of security for the entire supply chain, every element including the information flow must be consolidated into a whole.

Hence, concentrating on a collective security concept for the supply chain makes more sense than an individual solution. A collective security concept would serve as an orientation aid for companies that often invest considerably in security. Such a concept ought to be supported by detailed minimum requirements for individual links of the supply chain or even individual regulations for specific domains and special technical regulations if required. Moreover, such a concept must be regularly and easily updated.

### (2) Legislation

Security regulations for surface transport supply chains covering all transport operations and supporting processes between a good's place of manufacture and its destination are nonexistent. Following, selected European security initiatives will be described illustrating that until today (2007) merely proposals on hinterland and supply chain security are in place:

- Supply chain security (79/2006)
- European Critical Infrastructure (787/2006)

### (a) Supply chain security

The European Commission (2006) declared that this Regulation establishes common rules for enhancing land transport supply chain security in the face of threats of security incidents. For the purpose of this regulation supply chain means all the processes and operators involved in the preparation for transport and the land transport of goods from the production site to the point of delivery within the territory of the European Community. The measures laid down in this Regulation shall apply to any operator involved in one of the following activities:

- Preparation of goods for shipment and shipment of goods from the production site;
- Transport of goods;
- Forwarding of goods;
- Warehousing, storage or inland terminal operations.

The European Commission (2006) declared too that every individual business actor in the European transport market ([i] shipper, [ii] transport company, [iii] forwarding company and [iv] warehouse, storage facility or inland terminal operations [including inland ports]) has to fulfil proper security management requirements, which comprise all aspects of security:

- Physical security: All buildings and premises should be protected against unauthorised entry and protect against outside intrusion.
- Access controls: Unauthorised access to the shipping, loading and cargo areas should be prohibited.
- Procedural security: Measures for handling incoming and outgoing goods should include protection against the introduction, exchange or loss of material.
- Personnel security: Companies should establish an internal process to screen prospective employees, and verify applications, in full respect of the legislation in the areas of equal treatment and personal data protection.
- Documentation procedures: Companies should ensure that documentation is complete, legible, accurate and submitted in time.
- Information security: All information processes in the context of supply chain operations must be secured.
- Education and training awareness: A security awareness programme should be provided to employees including recognizing possible security risks, maintaining product integrity, and determining and addressing unauthorised access.

Currently, the proposal for a Regulation on enhancing supply chain security (COM(2006)79) has been put on hold by the European Commission, as the European transport sector did refuse this security approach due its

potential negative side effects on their businesses and the society. Until now, there is no final decision whether and if yes, how this initiative will be realised, apart from aspects which will be implemented in the modified European Customs Code.

#### (b) European Critical Infrastructure

The European Commission (2006) informs that the European Council of June 2004 asked the Commission to prepare an overall strategy to protect critical infrastructure. The Commission adopted on 20 October 2004 a Communication on Critical Infrastructure Protection in the Fight against Terrorism which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving critical Infrastructures (CI). In November 2005, the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP) which provided policy options on how the Commission could establish EPCIP and Critical Infrastructure Warning Information Network (CIWIN).

It declared that the proposal for a directive on European Critical Infrastructure (COM/2006/787) presents the measures that the Commission is proposing on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection. Because of the trans-national dimension, when investigating the weaknesses and vulnerabilities and identifying gaps in protective measures, an integrated EU-wide approach would usefully complement and add value to the national programmes for critical infrastructure protection already in place in the Member States and would add important value to the continued viability and wealth creation capabilities of the European internal market.

Currently, this proposal for a directive on European Critical Infrastructure (COM/2006/787) is under preparation and discussion.

#### (3) Effects on hinterland transport

Enhancing security in the transport sector covers two different levels. Firstly, the transport infrastructures (e.g. bridges, tunnels, terminals,...) need to be considered in the embedded framework of critical infrastructures. Secondly, the intermodal transport chains need to be protected covering all water- and land-based modes of transport and all business actors (shippers, transport operators, logistics service providers, port and terminal operators).

With regard to supply chain security the Federal Ministry of Education and Research in Germany (2007-a) informs that secure protection and transport of goods and guaranteeing the integrity of goods are vital to society and business. Terror attacks could affect the system in many places. An interruption in goods deliveries can cause considerable economic damage very quickly and

can lead to companies collapsing. Counterfeiting, contamination or misappropriation of the goods themselves can substantially disrupt social and business life. Every citizen can be affected if the supply of good is impaired. Securing the supply chains is of increasing significance for European countries export business and logistics location. Transport containers (such as letters, parcels, boxes, containers, tanks) may be misused for attacks or criminal purposes. The range of individual scenarios is very wide. Packing and containers allow prohibited activities to be camouflaged, attacks to be disguised and illegal objects to be moved internationally. Production facilities can be deliberately destroyed or manipulated. The flow of goods also contains items whose manipulation of theft could pose a great threat. This makes large container transport systems and logistics centres highly significant. Innovative solutions for their security are therefore extremely important to secure the supply chains.

Besides supply chain security, the security topic critical infrastructure exists. Regarding latter issue the Federal Ministry of Education and Research in Germany (2007-b) declares that in modern society, the various means of transport –road, rail, air, water – can be called its lifeblood. Their use has now become so finely balanced that even minor disruptions can have a far-reaching impact and cause considerable damage. If transport is cut off, it can become a disaster and destabilise society and business. The nodes in the transport system, such as airports, railway stations, dammed rivers and canals, bridges, tunnel and many more, are particularly vulnerable. It is absolutely vital to protect these neuralgic points. Therefore innovative solutions to protect transport infrastructures are a particularly important objective of the research.

### **3. Security concepts interlinking maritime with hinterland transport**

Efficient security concepts interlinking maritime with hinterland transport are basically non-existing nowadays. Consequently, accordingly with the European Intermodal Research Advisory Council (EIRAC) Implementation Plan several steps of implementation are needed to be realised for achieving the final objective of seamless secure transport flows.

1. Harmonisation of the Security Policy Framework: Different initiatives are taking place at national and European level to increase security in transport systems. The European Commission has launched studies to assess the effects of a new security directive for European surface transport, to be harmonised with the Port Security Directive and other European security legislations.
2. Physical security measures: Intermodal transport has specific requirements for physical security, ranging from inspection, and searches, to electronic sealing. All these elements are to be combined to strike the balance between security and effective-

ness.

3. IT-security: A common security related IT-infrastructure is needed to exchange and record security relevant data and information on transport operation.
4. Intermodal (hinterland) transport security: Analysis and assessment of transport security risk could lead to an estimate of the magnitude of investments that different players can support to increase security levels in divergent European regions/countries and different transport modes (road, rail, IWT, intermodal/multimodal transport).

### 3.1 Harmonisation of the Security Policy Framework

Security is, and tends to be during the next decades, a crucial factor in transport and logistics, which significantly affects the quality both of administrative and operational procedures. There are now many security initiatives on the table, like ISPS code, Regulation 2004/725/EC, Directive 2005/65/EC, CSI, electronic seals, RFID, “recognized secure operator or exporter/importer”, EU passports etc. The EU mainly adapts with a time delay relevant US or UN organizations, like IMO security initiatives, without presenting its strategy with priorities. This is an important political issue, which needs to be mentioned since it has a real impact in describing the research area within EIRAC. On the other hand, EU Customs Code imposes relevant checking procedures regarding transport and logistics. It also refers to “customs authorized shippers, operators, simplification procedures etc.” These initiatives gradually cause problems in all transport and logistics nodal points such as congestion, delays, piles of paperwork, increasing external and internal costs, conflict of interest between public bodies, operators and customers.

Different initiatives are taking place at national and European level to increase security in transport system. The EC has launched studies to assess the effects of a new security directive for European surface transport, to be harmonised with the Port Security Directive and the Airborne International Security rules. Studies aiming at achieving harmonisation of the identification of security critical transport infrastructures are in also progress. It is important that a European common policy to secure freight transport is developed and put in place, accompanied by suitable and common liability policies, by the creation of a forum for international cooperation and information exchange in the area of transport security, fostering the growth of a security culture by harmonising security policies of Member States, Accession Countries and main traders. One aspect of the harmonisation would be a Common Code of Conduct, containing the rules laid out for Intermodal players, how to behave and which security standards to observe, to become a recognised “Intermodal Secure Economic Operator”. EIRAC would define the Code of Conduct standards in line with other emerging standards on this subject.

### 3.2 Physical security measures

Intermodal transport has specific requirements for physical security, ranging from inspection, and searches, to electronic sealing. All these elements are to be combined to strike the balance between security and effectiveness. Thus, a major topic for research would be the development of new technologies for non-intrusive container inspection, characterised by short acquisition time, low cost, and high accuracy, such as the electronic seals, so that scanning delays at intermodal terminals should be minimised in order to maintain the competition position. The technologies are to be compatible, or developed in conjunction with the harmonised policies and the standard security IT infrastructure.

**Table 2: Physical security measures (EIRAC, 2006)**

Unit	Target	Today	< 5 Years	> 5 Years
Unit	Item		RFID	Nanotechnologies
	Package	Not in EU – Appearing in the US	RFID / Smart Box	Nanotechnologies, Enhanced Communication
	Pallet	Same as Packing, Bins have RFID	RFID / Smart Box	Nanotechnologies, Enhanced Communication
	Loading Unit	Cargo Protection Seals, Electronic Bolt Seals, Licence Plate RFID	Smart Container	Smart Dust
Vehicle	Lancio DAPP	Antitijft measures (biometrics, GPS etc.)	Navigation + Smart Container	Investigation on potential synergies between road security applications and intermodal
	Train	-		Investigation on potential synergies between rail information systems and intermodal
	Barge	New organisation	River Information Services (RIS)	-
	Vessel	-	Combined use of VTMIS	-
Site	Terminal	ID Cards	RFID at gates, enhanced biometrics, Gamma-ray scanners (drive through; mobile scanners) with risk analysis support, selection of inspections, alarming	Smart and Nanotechnologies, in combination with the IT Environment for security
	Warehouse	Same as above	Same as above	Same as above

Transport security combines preventive measures and human and material resources to protect transport infrastructure, vehicles, systems (including data transmission systems), cargo and workers against intentional unlawful acts. It should incorporate the supply chain, i.e. from the factory, shipping and recipients (end users) or point of export. Despite substantial improvements in recent years, laws and regulations governing such combinations of measures still lack harmonization both on EU and international levels, thus creating imbalances in their application. This is a major obstacle to achieve secure supply chains since supply chain security is only as strong as its weakest intermodal link.

Intermodal transport has specific requirements for physical security, ranging from inspection and searches to electronic seals. All these elements have to be combined to strike a balance between security and effectiveness. Thus, a major topic of research is the development of new technologies for non-intrusive container inspection (e.g. electronic seals) characterized by short acquisition time, low cost and high accuracy so that scanning delays at intermodal terminals would be minimized in order to remain competitive. Technologies must be compatible or developed in conjunction with harmonized policies and standard security IT infrastructures.

The management of information on the identity, current position and status of goods, loading equipment and means of transport as well as the real-time availability of this data in expediting systems is crucial when the transport of goods is unattended. The trend toward miniaturizing equipment as costs simultaneously decrease is opening new markets for intelligent logistics assets equipped with sensor systems and communication modules to optimize operational and logistical processes and meet security requirements. At present, the coupling of RFID systems for object identification with telematic modules is generating new products for the “secure chain of goods”. The functionality of the Smart Box and Smart Pallet represents a paradigm change from observing logistics assets from fixed measuring points to continuously tracking logistics assets even in intermodal supply chains.

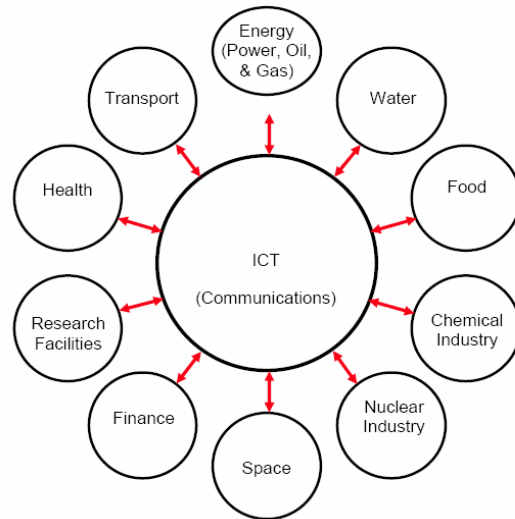
The Smart Box’s IT infrastructure is a security concept suitable for logistics to meet basic requirements of international supply chains incorporating hinterland transport Smart Box developments include reusable metal or plastic containers with RFID antennas and self-contained power supplies. Goods labeled with HF or UHF RFID are automatically recorded as container contents for ongoing inventory. A communication module transmits the continuously determined GNSS position of the container and every operation accessing it to the control center. Additional sensor elements determine the condition of goods. The Smart Box is an integral part of the newly opened DHL Innovation Center in Bonn (Germany).

### 3.3 IT-Security

ICT networks and systems are the nervous system of our modern technological society. The dependencies of other services such as electricity supply and water supply on ICT networks have grown ever more complex. In this context also the traffic and transport infrastructures have to be mentioned as they are also characterized as an vital element in the European business and society. Because of this interconnectedness and an increasing reliance on ICT networks, services critical to society and economy may become more fragile and may fall faster than ever before because of a major technological collapse of an ICT network or system, so European Commission (2007/a).

EIRAC members consider that a common security related IT-infrastructure is needed to exchange and record transport related information in a secure IT environment. Such IT environment shall cover all actors of the intermodal chain (terminals, carriers, shippers), be compatible with international customs standards, and use open standards technologies and procedures, to reduce investment costs. The IT infrastructure for Intermodal Transport Security shall be based on a common language or dictionary of terms applicable to all modes of

transport to ease storing, mining, and transfer of information. The solutions are to be envisaged in terms of functions, so that the infrastructure can be configurable and adaptable to technologies resulting from further evolution of ICT (Information and Communication Technology). By satisfying the requirements listed above, the IT infrastructure will add value to intermodal transport, rather than representing an additional barrier for its development.



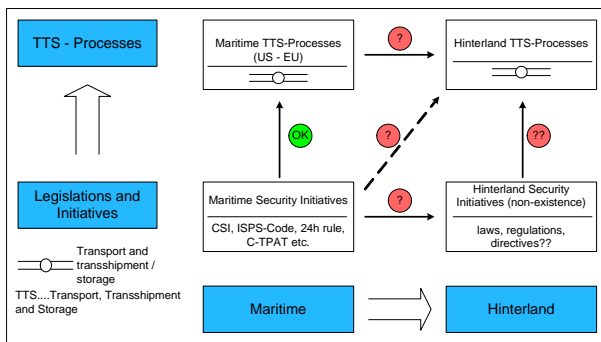
**Fig. 2: Infrastructure Dependence on Communication (European Commission 2007/b)**

### 3.4 Intermodal (hinterland) transport security

Transport security is the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems (incl. for data transmission), cargo and workers against intentional unlawful acts. It should relate to the supply chain, i.e., between factory gate, expedition point and recipients (end-users) or export gate. Although substantial improvements took place in the last few years, such a combination of measures still suffers from lack of harmonization in legislation and regulation at both EU and international levels, thus leading to unbalances in application. This is a major hindrance to achieve secure supply chain, as security in a supply is as strong as its weakest intermodal link.

Today, only EU sea ports have to come up with pre-determined US requirements and regulations inferring EU transport actions. Today (2007) other transport partners (here: hinterland / landlocked ones) – such as rail, inland navigation or road operators or logistics partners – (will) have to cope with derived deep or short sea security requirements as well. In the same manner, as today’s deep or short sea transport security processes will determine tomorrow’s hinterland or landlocked transport processes, existing maritime security initiatives will have a significant influence on coming up hinterland security regulations too. Besides all these short term activities, in the long run EU authorities will

set up adequate European initiatives considering special needs or requirements on planning and managing hinterland or landlocked transports, offering European transport partners reliable conditions for transporting commodities within European Union.



**Fig. 3: Security regulations affecting maritime and hinterland processes**

#### 4. Conclusions

Maritime ports are in a unique position. Maritime ports form the gateway of intercontinental traffic and cargo flows from/to European borders. Increasing transport volumes triggered by the reception of bigger ships lead to challenges both for operational partners and policy makers. Also capacities in hinterland/inland traffic relations are limited. The inclusion of sustainable surface transport modes (e.g. inland waterway transport [IWT] and rail), wherever possible, provides an attractive capacity on interlinking European traffic flows between inland with shore regions. Fostering the integration between maritime and (intermodal) hinterland processes is not only vital for cargo and/or information flows, but recently for security operations and processes as well.

Security in the European traffic and transport sector has been significantly modified. This circumstance can be primarily identified in the maritime sector, which – together with the air traffic sector – is affected by a higher degree than all other transport modes. It is obvious that especially the maritime sector has to comply with predominant security regulations either issued by international or European authorities.

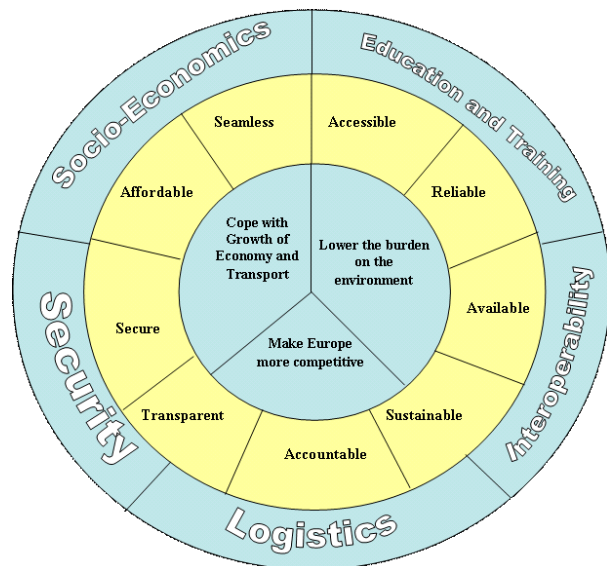
Sea ports are affected by current security regulations to the same extent as maritime traffic is, as they form the key transport and logistics node between maritime and hinterland processes. Consequently, sea ports have to correspond to almost the same security regulations like maritime traffic. Additionally, sea ports have to comply with other specific regulations, which have been issued primarily for them.

Hinterland transport operations are merely indirectly affected by the current security regulations until today. In most cases hinterland operators have to comply with

security regulations only, when either carrying out transports from/to sea ports or exporting commodities to overseas, here primarily to the United States.

#### 5. Acknowledgements

European Intermodal Research Advisory Council (EIRAC) is the intermodal industry's advisory council set up to influence investment in research and change in the European Intermodal Industry. The EIRAC has a membership of more than 50 key players in intermodal operation, terminal handling, freight village management, modal transport operation, forwarders, ports, equipment suppliers, and authorities. EIRAC has produced a Strategic Intermodal Strategic Research Agenda (SIRA), through a new and common vision for innovation and research until 2020, in conjunction with a business scenario. The SIRA is being led and produced by the intermodal industry for the intermodal industry, and is accompanied by its Implementation Plan of Innovation and Change, issued in December 2006.



**Fig. 4: EIRAC – Working Groups (EIRAC, 2006)**

EIRAC's primary mission is to establish and carry forward a Strategic Research Agenda that will influence all European stakeholders in the planning of research programmes, particularly national and EU programmes. Members share their personal visions of intermodal transport in 2020, identifying mainstreams of innovation, organising and prioritising needs for research that will be translated into the Intermodal SIRA, and into the relevant implementation plan. This will then be used as the instrument to direct EU and national resources to targeted research. The work of EIRAC Members is facilitated by CAESAR, a Coordination Action (CA) funded project for the purpose by the EU.

EIRAC has divided its task between five working groups (WG): Interoperability, Logistics, Security, Socio-Economics, Education & Training. Within these

working groups contributions both for the Strategic Intermodal Research Agenda (SIRA) 2020 and the Implementation Plan (IP) have been elaborated. Consequently, the working group security has developed missions, objectives and implementation cases for intermodal transport security covering all relevant modes of transport (road, rail, IWT, maritime) and security aspects (e.g. physical security, IT-security, security legislations, transport-logistics security).

## References

European Intermodal Research Advisory Council (EIRAC): Strategic Intermodal Research Agenda 2020, DECEMBER 2005

International Maritime Organisation (IMO): <http://www.imo.org/> (2007)

OECD: Directorate for science, technology and industry: Security in maritime transport, Risk factors and economic impact, Maritime Transport Committee, DSTI/DOT/MTC(2003)47/FINAL, July 2003, p. 6.

Rand Europe: Seacurity – Improving the security of the global sea-container shipping system, Santa Monica (United States), 2003, page 1

## Bibliography

European Commission:

[http://ec.europa.eu/information\\_society/newsroom/cf/document.cfm?action=display&doc\\_id=189](http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=189) (2007), page 156

European Commission: Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security, [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l\\_129/l\\_129\\_20040429en00060091.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_129/l_129_20040429en00060091.pdf), page 2

European Commission: Proposal for a regulation on enhancing supply chain security, COM(2006)79, Brussels, 2006, page 21ff.

European Commission: Directive 2005/65/EC of 26 October 2005 on enhancing port security, [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l\\_310/l\\_310\\_20051125en00280039.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_310/l_310_20051125en00280039.pdf), page 1-2

European Commission: 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, Brussels, 2007, page 2ff

European Commission: White Paper: European transport policy for 2010: time to decide, Luxembourg, 2001

European Commission: Directorate-General for Energy and Transport: Directorate G – Maritime Transport and Intermodality: The Director: Consultation Paper – Freight Transport Security, Dec. 2003, Brussels, page 3-4.

European Commission:

[http://ec.europa.eu/information\\_society/newsroom/cf/document.cfm?action=display&doc\\_id=185](http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=185) (2007), page 1

Global Security:

[http://www.globalsecurity.org/security/systems/carg\\_inspect.htm](http://www.globalsecurity.org/security/systems/carg_inspect.htm) (20.09.2006)

Maersk Logistics:

<http://www.maersklogistics.com/sw18204.asp>

The Federal Ministry of Education and Research in Germany (a): Research for Civil Security, An Inventory: Research Landscape and Contacts, Bonn/Berlin, 2007, page 101

The Federal Ministry of Education and Research in Germany (b): Research for Civil Security, Programme of the German Federal Government, Bonn/Berlin, 2007, page 28

US authorities: Coast Guard and maritime transportation act of 2004, public law 108–293—AUG. 9, 2004, page 1028

US Customs & Border protection: Securing the Global Supply Chain Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan, 2004, page 12.

U.S. Department of Homeland Security: Office of Inspector General: Office of Inspections and Special Reviews; February 2006 (revised)

U.S. Department of Homeland Security: US customs and border protection, Sept. 2006, [http://www.cbp.gov/linkhandler/cgov/border\\_security/international\\_activities/csi/csi\\_fact\\_sheet.ctt/csi\\_fact\\_sheet.doc](http://www.cbp.gov/linkhandler/cgov/border_security/international_activities/csi/csi_fact_sheet.ctt/csi_fact_sheet.doc)

United States Government Accountability Office: Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure, 2005, page 22