EVALUATING THE IMPACT OF SECURITY MEASURES ON CONTAINER SUPPLY CHAINS

Senior Assistant Prof. PhD Varbanova A.
Faculty of Shipbuilding – Technical University – Varna, Bulgaria

anneta_varbanova@hotmail.com

Abstract: *The present article analyses the development and impact of the container security initiatives on maritime supply chains. Security issues concerning container liner shipping require complex approach and application of integrated IT systems on national and international levels. During the last two decades various initiatives have been applied to ensure for higher level of security of container transportation. The background and aim of these initiatives are studied in detail and their effect is evaluated. The results show that container transportation still has vulnerable nodes and the application scope of security initiatives is to be widened despite the high costs.*

Keywords: CONTAINER LINER SHIPPING, CONTAINER SECURITY, PORT SECURITY, MARITIME SUPPLY CHAIN

1. Introduction

During the last two decades several international regulations have been introduced focusing on security issues of containerized cargo flows. These are the International Ship and Port Facility Security (ISPS) code, the Container Security Initiative (CSI), the 24-hour Advance Vessel Manifest Rule. To support the global supply chain as concerns proactive approach for incidents prevention and tracing of containers, ports and logistics stakeholders have introduced new technologies based on real-time information systems [4]. The transportation of containerized cargoes requires efficient supply chain management and relevant security measures. European ports have been given the opportunity to establish the required security level in response to newly set international standards. The European Shipping Containers Surveillance system, implemented via various EU funded projects includes a number of recommendations – standardization, national regulations, policy guidelines. The present article analyses the effect of the global container security measures. The processes of logistics chain of container transportation are presented, outlining the vulnerable nodes as concerns security issues. The positive and negative effects of the security measures are assessed via quantification of direct costs to logistics stakeholders.

2. Structure of container supply chain and security issues

Container supply chain is characterized by complex interactions between numerous subjects, production areas, regulating bodies and polices. At the beginning of the container supply chain are the shippers who require the services of intermediaries that will ensure for the international transportation of containers including maritime transportation. At the other end of the container supply chain are the consignees who require timely and quality delivery of goods. Most of the container cargo flows are initiated on the basis of commercial interactions and relations between sellers and buyers. In most cases, however, it is the shipper who disposes of the exact information about the type and quantity of cargoes shipped in containers. The latter is of fundamental importance as concerns the security of container supply chains. Due to the relatively medium-scale of the shippers' enterprises, these companies do not have access to resources for increasing the supply chain security level.

Forwarders, on the other hand, have better overview of the supply chain but their "hybrid" role both as carriers for their clients or shippers for carriers can be a prerequisite for hindered access to information regarding the cargoes. Forwarders companies are predominantly medium-sized companies that are not able to fulfill the costly security measures.

The surveillance and monitoring of containerized cargo flows is the responsibility of each governmental body as well as of the customs office. Customs are responsible for securing that containers and the cargoes are customs cleared during exports, transit and import procedures.

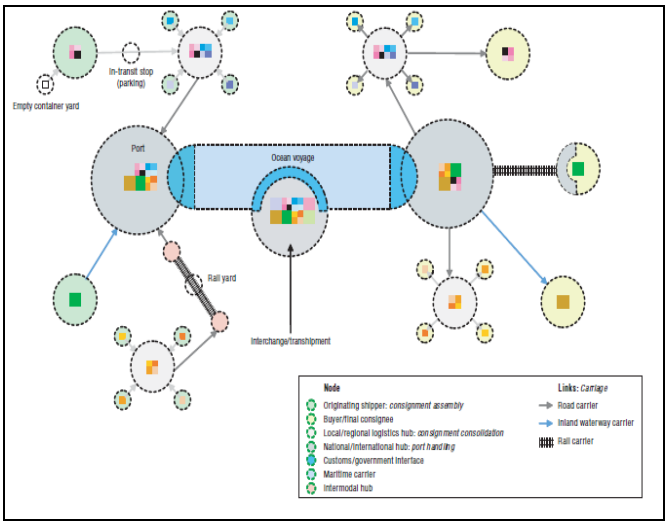
The security of the container supply chain is responsibility of all participants and any disruption of security can compromise the entire supply chain. The vulnerability of containers due to environmental factors is related to railways warehousing, road transport stoppages, during storage and loading at container terminals. As concerns these vulnerable nodes all efforts should be focused on ensuring the physical safety of storage areas and minimization of unauthorized access. The monitoring of containers transportation should be implemented within "real-time" environment and at the right moment, i.e. there should be reliable information at any moment about the location of the containers.

The physical flows of container supply chains constitute the movement of the containers and represents the material flows from a security point of view. In general, the network of nodes and edges in containers supply chains consists of several processes (Figure 1):

- consolidations of cargoes;
- transportation to the port of loading;
- handling at the port of loading;
- transportation by sea;
- handling at the port of discharge;
- land/inland waterways carriage to the consignee.

More efficient routing of containers with minimum stoppages during transportation and decreased storage time increase the safety of cargoes transportation and ensure for higher revenues for all participants.

Figure 1: *Container supply chain for exports [2]*



3. *Container supply chain security measures*

Container supply chain security measures can be classified as follows:

- focusing on the monitoring of the container content;

- focusing on the containers integrity;

- aiming at the ensuring of safety of the environment during the transit and handling of containers;

- related to the monitoring of container transportation within the entire supply chain;

- ensuring and usage of supply chain information.

Being a complex structure, each container supply chain element is aiming at optimization of its own processes According to the well known principle in logistics management, the aggregating of individually optimized relations in some cases results in non-optimal supply chain. Non-charmonized practices, incompatible operations and information management systems, uncoordinated regulations, both on national and international level, can lead to vulnerability of the security system due to lack of coordinated approach.

As concerns the security of physical flows the following should be considered:

- the containerization point is of prime importance as concerns security since it is the last point where the contents of the container can be visually identified and compared with the respective invoice or waybill. Until the moment of decontainerization all information regarding the content of the container will be evident only in the cargo documents (freight manifest, Bill of Lading, etc.)

- containers are most vulnerable when they are standstill which means that security measures are most important in those nodes where containers are being handled or stored;

- crossing of international borders includes extensive customs control that leads to potential delays;

- most of the containers traffic transits through at least one sea port which levels of security and relevant security measures are at a different level.

There are two major types of physical surveillance of containers: X-ray scanning (non-intrusive inspection) and direct physical examination. The latter usually involves at least 8-10 hours per container which can lead to potential delays for the entire delivery.

The Container Security Initiative is structured around the concept of "pushing the border back", i.e. identifying the security risk at the point of origin and before shipment and serving as protection against pertaining risks during containers transportation. Presently, there are over 50 ports that have been approved for applying the Container Security Initiative (SCI) as shown in Figure 2.

As of April, 2008 the European Union and the USA have signed an agreement for activization and expansion of cooperation in customs procedures and mutual cooperation as concerns containers security. The agreement concerns cooperation for ensuring of containers transportation safety and related issues and is applicable to all containers carried by sea, irrespective of their origin, that are imported, handled or transiting through EU and USA.

The container security initiative (CSI) consists of the following four elements:

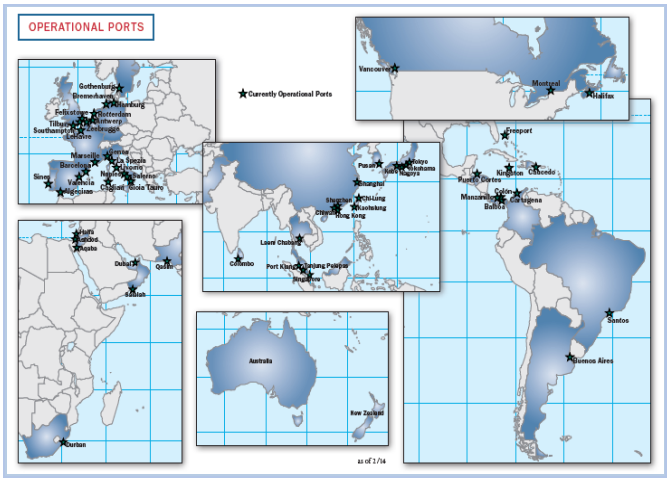
- high-risk containers are identified via automated information;

- containers are pre-screened for high-risk identification;

- usage of special equipment for detection and screening of high-risk containers ensuring of inspections without delay;

- usage of smarter containers that are tamper-proofed [6].

Figure 2. *Ports, applying the Container Security Initiative [6]*



The "24-Hours Rule" is based on automated information for identification of higher risk containers. As of 2002, all carriers are obliged to submit electronic cargo manifest to the US Customs before cargo loading. The mentioned rule is also applicable to transit and empty containers as well as bulk and conventional general cargo shipments. The cargo manifest is the document that legalizes any cargo carried by a seagoing vessel and contains information about the shipper, consignee, notify party, port of origin, port of destination and cargo description. In this way customs authorities are closely monitoring the shipment content along with the time periods needed for the container transportation. The container is being tracked if risk is identified or dangerous goods are carried in the container. The mentioned information, transmitted electronically, is used both for exports and imports. It is the responsibility of the carrier to ensure for information provision which is accurate and complete and is submitted at the required time. Some states do not disclose information contained in cargo declarations for security reasons until the process of cargo manifest filing is completed – the relevant information might be published only after loading is completed and the vessel has left the port.

Screening systems usually use x-rays, gamma-rays machines and GPS. The mentioned technology allows for fast inspection without delay apart from the technological time needed for the screening. This type of equipment can identify specific materials which can potentially pose a risk to the environment.

4. Cost analysis of container supply chain security measures

The costs pertaining to the implementation of security measures can be indirect and direct. The latter are the capital costs, necessary for the design and implementation of the security network:

- purchase of new equipment for physical structure protection;

- adoption and/or implementation of security regulations;

- implementation of security policies and regulations;

- employment of trained security personnel.

Costs that are classified as indirect are the costs related to the system operations: equipment maintenance, application of efficient management strategies, response costs to incidents, costs related to management and operations recovery and reconstruction of infrastructure.

For the ocean carriers the costs include the following elements [1]: costs for setting up a new system for documentary transactions, costs for increased communication, personnel training, increased labor costs (cargo handling and inspection, operations of special equipment), usage of security-related equipment. For example, vessels are equipped with Automatic Identification System (AIS). Carriers also use software for monitoring and tracing of container movements for preventing incidents and illegal actions. As for specific technologies being used - Global Positioning System (GPS), Radio Frequency Identification (RFID) and electronic seals of containers also enhance the tracking of containers. It could be necessary that special security equipment is installed on board the vessels to enhance the global security measures.

The costs of security measures that impact the entire container supply chain are related to:

- time delays due to security inspections, whereas the costs will be higher at the very beginning of the transportation process; delays in the delivery time will eventually lead to penalties to parties and/or damages due to decreased cargo quality;

- costs for providing cargo manifest in advance, whereas this requirement is based on the "24-Hours Rule"; although the information contained in the manifest is not disclosed at an early stage same could be used for illegal purposes and losses related to the latter are borne by several participants in the supply chain;

- the introduction of additional state taxes related to the design and maintenance of the security infrastructure and equipment;

- increased insurance premiums despite the applied new security systems on board ships and in ports.

In addition to the expected higher revenues, the most important benefit from increased security measures is the increase of cargo flows to and from ports applying higher security level system.

Risk analysis and risk management, performed by the various participants of the container supply chain, will enhance the evaluation of potential gains and reduce the cost of investments. Decision makers are to explore the fixed costs for application of the international regulations, increase costs for communication exchange along with increase of operational expenses, inspection and personnel training cots. It should be noted that the economic benefits of increased security measures for container supply chains are more evident in the long run therefore strategic management is to implement such measures.

According to [3] the cost benefit analysis of a new automated cargo manifest estimates direct saving to American importers only at USD 22.2 billion over 20 years and savings of USD 4.4 billion for the American government over the same period.

The CSI requires that all foreign states invest in special equipment (screening, detection) and provides guidance to port management via trained personnel. However, recent evaluations have shown that the overall costs of increased security measures will be borne by the clients and will be calculated as additional costs per container. Depending on the type of port management, the state or the municipality will initially invest in the required special equipment which returns are calculated on the basis of increase of prices for shippers, carriers and port services and, finally, of the final prices of goods.

Given the higher costs of security measures application the less developed countries/ports will bear the largest burden of market share loss. Due to the high competition in the shipping market, both tramp and liner, these companies/ports will inevitably face reduced revenues and loss of market position. According to [5] the CSI program proposed by the US will be difficult to implement by some small developing countries because the cost per port for that program varies between USD 1-5 billion. Table 1 presents an approximate estimation of related costs for the implementation of obligatory and optional security measures.

Measures		Initial costs (approximate, mln USD)	Yearly cost (approximate, mln. USD)
Port facility assessment	Security	27,9	8
Port facility plan	Security	N/A	N/A
Port facility officer	Security	N/A	N/A
Port training	Facility	N/A	N/A
Port facility equipment/staff	Security	N/A	N/A
24-Hour Automated Manifest System	Security	281.7 to 10 000	281.7 to 10 000
Container Security Initiative	Security	N/A	N/A

Table 1. *Cost of container supply chain security measures [7]*

When implementing only the obligatory requirements as per the IMO conventions (for example, ISPS), apart from the optional requirements (CSI), less developed countries will inevitably face decrease of cargo flows and cargo turnover at ports as supply chain participants would prefer faster and more secure transportation. Even in the medium run the latter will distort the international trade patterns.

5. Conclusion

The present paper analyzes the framework of security measures in container supply chains, outlining the strengths and weaknesses of the mandatory and optional security measures. The existing security measures aim at the protection of international and national interests and ensuring of safe environment.

All the participants of the container supply chain are challenged by the fact that that there are no universal standards concerning the container transportation apart from the mandatory regulations of IMO at ports and for sea carriage (ISPS, SOLAS). The other edges of the container supply chain – road and rail transport, as well as inland waterways, are still the vulnerable parts of the system.

The available solutions for security enhancement of container supply chains, however, involve certain delays in cargo flows. All participants should bear the cost and responsibility of the applicable measures. Shippers are responsible for the containers content and provide the relevant info via automatic cargo manifests transfer to the national customs authority as per the "24-Hours rule". On the other hand, ocean carriers are responsible for vessel's deviation from the customary route and are obliged as per ISPS code to provide advance ships' arrival information to port authorities. The strict security procedures of the CSI will lead to delays in the transportation process especially for carriers and shippers. A detailed analysis has been made regarding the cost of the security measures and its effect on the container supply chain. The results show that the benefits from increased security measures are higher for all supply chain participants, allowing for protection from usual hazards during the transportation process.

References

1. Erera, A. et al., 2003, Cost of security for sea cargo transport, White Paper, The Logistics Institute – Asia Pacific, National University of Singapore, Singapore

2. OECD, 2005, Container Transport Security Across Modes, European conference of ministers of transport (ECMT)

3. Organization for Economic Co-operation and Development (OECD), Report in Maritime Transport

Committee 2003, Security in maritime transport: Risk factors and economic impact., OECD publications, Paris

4. Scholliers, J., A. Permala, S. Toivonen, H. Salmela, 2016, Improving the security of containers in port related supply chains, Transportation Research Procedia, 14, pp. 1374 – 1383
5. United Nations Conference on Trade and Development (UNCTAD), 2004, Container Security: Major initiatives and related international developments, Geneva, United Nations
6. US Customs and Border Protection (CBP), 2006, Container Security: Fact sheet, Washington, CBP publication
7. World Maritime University, The Maritime Commons, Digital Repository of the World Maritime University, World Maritime University Dissertations, 2006, Intermodal shipping: an examination of the security framework with emphasis on container security, M. Abdou