JOURNAL OF MARITIME RESEARCH

Vol XVII. No. I (2020) pp 52–64

ISSN: 1697-4040, www.jmr.unican.es

The ISPS code gap requirements costs and related financing by the implementation in Saudi Ports

Akram Elentably[1]

ARTICLE INFO

Article history:
Received 17 February 2020;
in revised form 1 March 2020;
accepted 16 March 2020.

Keywords:
ISPS, Port Ship Investment, IMO Security, Cost assessments.

ABSTRACT

Without transport, there is no economic development, and the more efficient the transport, the better development proceeds. Especially since more than 90 per cent of world trade annually is transported by sea with the possibility of increasing the percentage mentioned annually which led to the trend towards increasing the size of ships (especially in container trade) due to the impact of the ever-increasing globalization, so there are requirements to secure the port facilities Satisfactory While these facilities must be properly secured, so-called logistical challenges arising from the accelerated shipping traffic around the world have also emerged. This has resulted in the development of service levels for ships operating on international flights. Therefore, multiple port ports should include full implementation of ISPS requirements. Contracting Governments decide to what extent the Code can be applied to port facilities within their territory, which are sometimes binding and required to serve ships involved in international transport. The immediate challenge for the port community is how to finance the costs of implementing ISPS, and ways to integrate and adjust them according to pricing and marketing strategies while maintaining market shares and achieving reasonable profit margins. The long-term challenge involves adjusting relationships with suppliers and customers to ensure flexible and competitive supply chains, capable of overcoming risk threats while continuing to deliver value to customers and users.

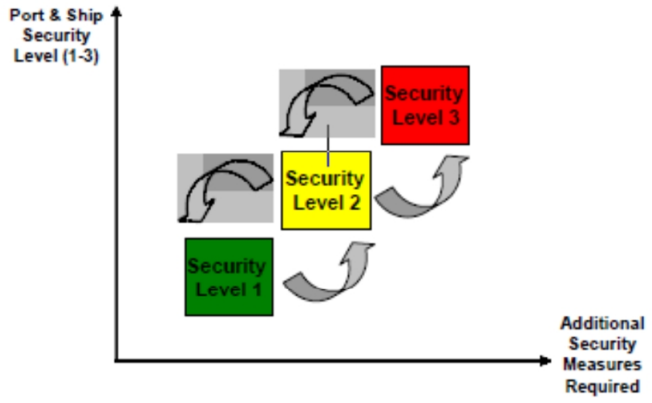
1. Introduction.

ISPS is content that includes imperative measures adopted by IMO to improve the security of ships and port components. The main objective of these measures is to establish an institutional structure through which predictions of risk assessment can be made, thereby enabling Governments to examine the gap between what is required and what is available in order to control threats to ships and seaport components in order to achieve balanced security levels and assess the magnitude of efforts. Required. The ISPS code is mandatory for 148 countries, grouped under the SOLAS (Safety of Life at Sea) Convention. The introduction of the ISPS Code has raised many inquiries and assumptions as well as some financial implications that have affected the cost structure of ships and ports. It was a truism that the ports constructed the fence around their units. Later, however, I discovered that the security fence was not enough to prevent danger from the port's components.

Basically, the ISPS Code adopts the strategy to identify appropriate safety efforts, where a risk assessment should be conducted in each specific case. However, it seems that the IMO has never been satisfied with its principles being represented solely in this security fence, with loopholes that could serve as a conduit for risk sources as well as identity checks, and misinterpret the systematic treatment of seafarers' rights. Existing within the Container Security Initiative (CSI) or particularly sensitive cargo care, regularly escapes a similar method to ascertain the level of investigation. Coordination and arrangement with ISM has been instrumental in activating security requirements. IMO has recognized the need for complementarity and coordination among the basic requirements of the ISPS Code and the Ship Security Plan (SSP) so that duplication of efforts can be avoided. Security is certainly great for creating awareness of threats to ships and ports. (Chiptek, January 2007)

[1]Ports and maritime transport department. Maritime Studies College. King Abdul-Aziz University.

Figure 1: The levels security measures.



Source: Author.

As indicated, the motivation behind the Code is to provide a reliable institutional structure for risk assessment, enabling governments to balance changes at risk by ensuring appropriate security levels and related safety efforts, which are taken by either the legislature, transport organizations, ports or some other elements that are responsible for protecting the oceans. In this regard, the port has three basic tasks, for example:

To complete the Port Facility Security Assessment (PFSA), which should address the accompanying components:

- Physical security.
- Structural integrity.
- Individual security frameworks.
- Procedural methods.
- Radio.
- Telecommunications and IT frameworks.
- Various facilities and areas that pose a threat to persons, property or tasks within port units.

Prepare the Port Facility Security Plan (PFSP), which should be separated through the Port Office Security Association, build effective communication of the Association with other relevant sources of answers and ships in the port, detailing the basic physical and operational safety efforts of three diverse levels of security, and visualize strategies That reveal the appropriate contacts, and

Appointment of the Port Facility Security Officer (PFSO), whose tasks include directing a comprehensive security study of the Port Office, improving, supporting, implementing and practicing PFSP, conducting regular security audits, ensuring satisfactory preparation of the security workforce, and ensuring security through properly tested, functioning and monitored devices , Organize the use of PFSP with enterprise security officials and ship security officials.

Section A of the Code is mandatory for each port office that handles cargo ships of 500 tons or more on international voyages. Port offices and units in this case should follow the ISPS code (about 6500 port offices around the world). The immediate verification and testing of the port network at that stage is the way to support the costs of using ISPS, integrating and changing them to estimate and enhance methodologies while maintaining parts of the overall industry and generating reasonable net revenue. The long-term challenge involves adjusting relationships with service providers and customers to ensure adaptable chains that are appropriate to overcome disability risks.

Operators or customers pay for the instructions and transfer them to customers in the inventory network;

Port authorities bear all expenses from their spending limit at no additional charge to clients; other public bodies bear all expenses from the national expenditure plan (eg citizen pay) at no additional charge to customers, or Costs are shared among all beneficiaries as much as open prizes or as a private open association. There is no doubt that the study of the expenses of coordinated safety efforts towards ports is more complex than those rules directed to ships. In addition to the fact that ports are exceptionally divergent in terms of hierarchical, operational and administrative frameworks, the safety efforts they focus on in addition contrast with time, space, extension and nature, as noted above in the ISPS code clarification.

The process of evaluating or anticipating projects that will be required and with any amount of stevedoring charges will increase as a result of using the ISPS code. For example, port security expenditures in some ports have been estimated to be in excess of US $ 200 million, the equivalent container of US $ 30 per TEU and per ton of general cargo at around US $ 11 per ton.

To know the expenses as a result of the implementation of ISPS, we must collect cash data on investment and operational or current expenses. At any point is accessible, with quite a distance from the speculations of interests in security that were made before the submission of the ISPS code, and those that were clearly made as a result of the implementation of ISPS. Moreover, note the application of the additional projects required for the safety code to the expenses per TEU and expenditures per ton

This paper will cover the accompanying views:

- Completion of procedures aimed at meeting ISPS law;
- Support costs by ports.
- Direct expenses incurred on port clients.
- Direct expenditures resulting from Contracting Governments;
- Support costs required to implement urgent rather than forward aspects.

2. The goal of the ISPS principle in shipping.

The ISPS safety code is mostly concerned with the security parts of the ship, sailors, ports and port workers, to ensure that preventive measures are taken if or when a security risk is anticipated. Key points in the ISPS include:

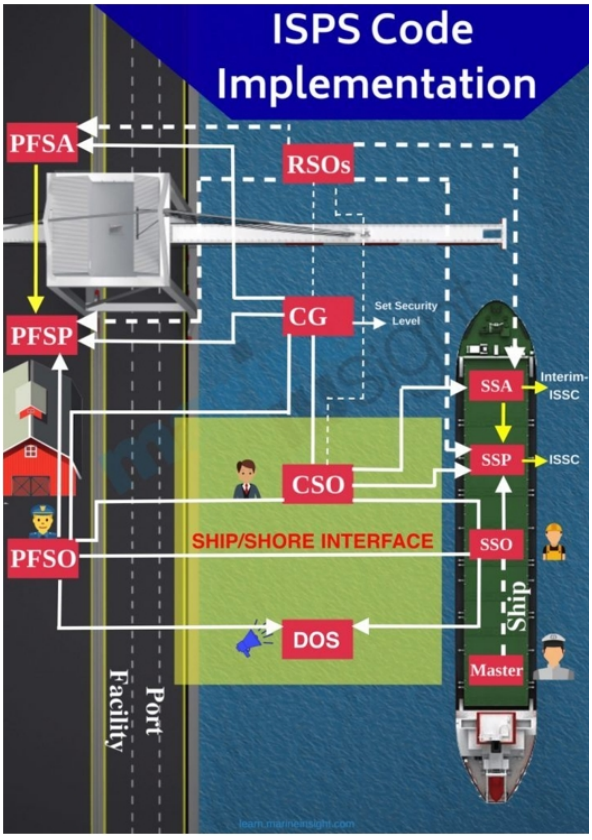
- Examine personnel activities and shipping activities.
- Ability to distinguish various security risks on board the ship and at the port and achieve the necessary measures according to the circumstances.
- Determine the safety level of the vessel and identify different obligations and capabilities at varying safety levels.
- Create the separate functions and obligations required to implement the code.
- Identify, compile and fulfill the tasks and obligations of port State and proven officials to deal with global peripheral security risks.
- Gather information from everywhere throughout the maritime business regarding security risks and achieve the necessary approach to deal with them.
- Ensure the handling and flow of security-related data collected with comprehensive regulation of port and ship owners.
- Provide the methodology for security assessment to develop plans and methodologies to respond to changing security levels.
- Acquire the capacity to detect deficiencies in the ship security and port security plan and take measures to improve it.

3. ISPS code requirements.

The ISPS code incorporates various operational requirements so that it can achieve certain destinations to ensure the security of ships and ports. The following components are therefore important:

- Compile safety data from government offices contracting the SOLAS Convention and signed on the Safety Code.
- Evaluation of data acquisition methods.
- Commitment to publish appropriate safety data.
- Identify the best possible correspondence agreements for ships and port offices to ensure data flow without problems.
- Avoid unwanted sections in port offices or on board a ship and other designated areas.
- Avoid unauthorized weapons, flammable devices or explosives for ships and port offices.
- Give different scenarios to raise the alert in the event of any security presence or a survey of potential security risks.
- Achieve the legitimate security plan on the port and ships that depend on the assessment of security and necessities.
- Plan and execute the preparation, ships and activities of the ship and port team so that they know the security plans and the need not to postpone the proceedings if there should be a real risk.

Figure 2: The stages of ISPS Code Implementation.



Source: Author.

We noted from the above figure that:

The ISPS code consists of two parts and three degrees of security.

SECTION A. These are mandatory arrangements that discuss the work of security officials in transport institutions, ships and port offices they name. In addition, this covers various security issues to be taken into account in the security arrangement to be achieved in ships and port offices.

Part B - These are the recommendation arrangements that give guidance and suggestions on how to arrange and implement the above security plans. Security levels are achieved by the Port Authority with management specialists. The safety of the port office should be facilitated with the ship. The three degrees of ISPS security are:

Security Level 1 - Typical - This is the level at which ships and port offices operate under normal conditions. The lowest defensive estimates will be maintained consistently.

Security Level 2 - Increased - This level will be applied any time there is a significant risk that can be enforced from the

security chain. At this level, additional safety efforts should be achieved and kept up to date. This time will be allocated by security professionals on the ship or at the port office.

Security Level 3 - Excellent - At this level, it is seen that a safety loop cannot be avoided and the specific security efforts must be achieved and this timeframe should be met. At this level, security professionals will work closely with government offices and are likely to adhere to explicit conventions and guidelines.

4. Meaning of ISPS code for ships:

Loading vessels are unable to face security risks because they rarely transport any insurance weapon in the event of a real attack. On the other hand, theft, or fear of attacking the crew and many of the continuing dangers that are repeated or likely to be repeated to the ship and its group. Improved ship safety will therefore be required in order to discriminate and take preventive measures against such security incidents.

The organization is responsible for auditing and supporting the ship's security plan, which will similarly include any revisions to the old plans and so on. The organization should also train its official rather than formally adopt transport security and the ship's security assessment will be transferred and made available locally by these confirmed officials. An appropriate assessment of the SSP by a confirmed official is essential to discovering deficiencies and upgrading the existing service provider. The assessment, exploration, recognition and confirmation of the ship's security will also be archived. At the same time, in parallel, each ship must be provided with an approved security plan for the ship confirmed by management.

4.1. ISPS Ship Code includes:

4.1.1. Organization Security Officer (CSO).

His responsibility includes assessing ship security and reviewing locally available to confirm progress in using the ship's security plan according to the ISPS code. In case of any deficiency, CSO is able to manage all inconsistencies and change SSP according to insufficient requirements.

4.1.2. Ship Security Officer (SSO).

He discharges his role in the security responsibility of the ship on board the ship, which is responsible for the entire crew who is also entrusted with the security duties of the ship according to the ISPS code. SSO is also responsible for carrying out repetitive exercises in accordance with ISPS code and SSP.

4.1.3. Ship Security Plan (SSP).

It is an arrangement maintained on a ship that indicates the commitment of team members at different levels of safety, what they do and what they must take in an alternative type of safety risk. SSO is able under CSO to execute the delivery of the locally available ship safety plan.

4.1.4. Ship Security Alarm System.

Various types of security devices are kept on board, including a metal search tool to check the person entering the ship. As of July 2004, the vast majority of ships provided the ship's Security Alert System (SSAS) in accordance with ISPS standards and the beach authority's warning of security risk.

4.1.5. Activate ISPS security level.

SSO's commitment to implement the onboard safety level corresponds to the level of security set by the government for both the original port and the expected port of the state. Similarly, a static reaction to the port state must be performed when the security level is "Level 3".

5. ISPS code for port facilities.

Port offices need to ensure that each office is protected from any kind of risk that may arise from both land and water. They also need to inspect ships frequented by their ports. It is the port office that distinguishes the safety levels to be achieved on ships in its territorial waters. The port authority is responsible for preparing the port facilities safety plan. In addition, the Port Office Safety Assessment is an essential part of establishing and updating the Port Office Safety Plan. The assessment is usually surveyed by the administration responsible for transport and port development for that country.

5.1. The ISPS code for port facilities includes:

5.1.1. Port Facility Security Officer (PFSO).

PFSO is a designated government official responsible for the implementation of PFSP and to infer the safety levels of the wharf and ships at the breakwater. It has the ability to guide the assessment of port office security.

5.1.2. Port Facility Security Plan (PFSP).

It integrates plans and moves at different security levels. The functions and obligations are integrated into the PFSP. The step to be performed is also performed at the hour of any security breach in PFSP.

5.1.3. Security equipment.

Access to less secure security devices such as a scanner, metal detector, etc. must be consistent with the port office to avoid security breaches inside the port.

5.1.4. Security level activated.

Safety levels are achieved by the Port Authority. The level of safety received at the port office should be marked to regulate ships in order to take the necessary and necessary measures.

6. ISPS code difficulties:

Each guideline is accompanied by its own difficulties. Human rights are likely to be the biggest concern with the ISPS symbol because they legitimately affect the prosperity of seafarers. In terms of impact on coastal vacation, it is always a process that is considered to be a major pressure on the ship's crew, and due to security risks, many countries do not allow such beach vacation.

Implementing the safety level on the ship is an additional activity, which is hard. In order to increase the level of safety, ports bear many of the costs of training courses for their employees, in addition to delaying the activity of the payload and when the level of safety is at its highest level, the remaining port of the ship will increase as all shipments are examined when they are contrasted with the low level of safety (1 and 2). The range of shipments is checked only for security reasons

Some ports do not allow charging tasks under Security Level 3 until the level is checked and verified.

7. Favorable conditions for ISPS code:

- ISPS plans to build the welfare and security of the ship thereby reducing risk,
- Better control of the cargo stream, and individual access,
- Better documentation methodology (because it has standard strategies everywhere),
- Safe working conditions making it simpler for sailors and port workers,
- The application of the code allows additional work for seafarers where security-related tasks are added to the routine work schedule,
- Additional office work to achieve accreditation requirements,
- Increase in ship operating expenses for ISPS implementation and increase in port costs (port size increases) if security level is higher,
- More regulatory work.

8. The present Status of the ISPS Code in the majority of ports considered.

8.1. Port Class A1.

To facilitate the follow-up and identification of the various ports centers in Asia, including the Arabian Gulf region and Saudi Arabia, it has been divided into three groups, where the Ministry of Transport is the contracting government component for port security. Through this category, the Ministry has established a security committee specifically appointed to arrange ISPS rules. After the national ports were assured to accommodate ISPS requirements, it was completed that. Harbor Master at port A1 is the Port Facility Security Officer (PFSO). PFSO is responsible for the various units in the port under this category: such as container terminal and port area, and each office has a deputy head. The PFSO is also responsible for the Port Security Committee which includes one or more Deputy, Port Security Director and Port Police Agents, Immigration Department, National Bureau of Investigation, Army and Navy. The Director of Port Security is responsible for following up the tasks of the members of the Safety Authority through four groups granting security commitments 24 hours a day, seven days a week. Some port security updates that have been proposed in the overall port security assessment have been implemented and work towards arranging other updates. However, they were still dissatisfied with the identification and application of safety code standards, and are still not eligible for certification, but to protect them, they were Some of the activities proposed in the PFSA are still going on, for example, a new fence around the port.

8.2. Port class A2.

The Department of Transportation (MOT) is responsible for port security. He is also a Port Facility Security Officer (PFSO). He reports to the Director General of the Port Authority (PA), who then reports to the Ministry of Transport. PFSO is the Director of the Security Committee which additionally includes representatives from the Port Police, the Stevedoring Association, Delivery and Customs, Immigration and Army organizations. PFSO capabilities act as port security manager and Harbor Master - the port manager's working time is generally divided into equal parts between the two functions. In general, few of the port security reforms identified by the PFSA have been implemented. The remaining obligations arising from the periodic assessment of safety code requirements are still being implemented. It also seems that the case of using ISPS Code in the Port A2 class is completely inadequate. Consequently, the port will not obtain its certificate of compliance in many different countries around the world, mostly for the following reasons:

- Overall implementation not completed (but in progress),
- Insufficient access control, and
- Limited load control.

8.3. Port A3 class.

The Directorate of Maritime Affairs (DMA) is the administrative authority responsible for the security of national ports. Port A3 Risk Manager is Port Facility Security Officer (PFSO). For security, downtime issues, PFSO notifies the DMA. The security officer for each of the designated ISPS offices shall be deemed to be a Deputy of the Authority. The port has formed a port security committee comprising port representatives, police, customs, immigration, defense, fisheries, municipality, security association, DMA, port user associations and port health. The committee meets at regular intervals. The chairman of the port security committee is selected for a specific period by the committee members. Public security in the Port A3 class is redistributed to a private security organization. In return for

fixed annual expenses, the port also has about a number of full-time workers whose main task is to supervise the temporary workers' safety staff. Port A3 has implemented port security redesigns proposed through the PFSA. A specialist for implementing ISPS Code in the Port A3 class is acceptable. The Port A3 class will receive its compliance certificate in most countries around the world. The shortcomings associated with Port A3 safety efforts are as follows:

External edge fence. The planned expenditures were about US $ 500,000. The implementation obligation was implementation on the spending limit for the next 1-2 years.

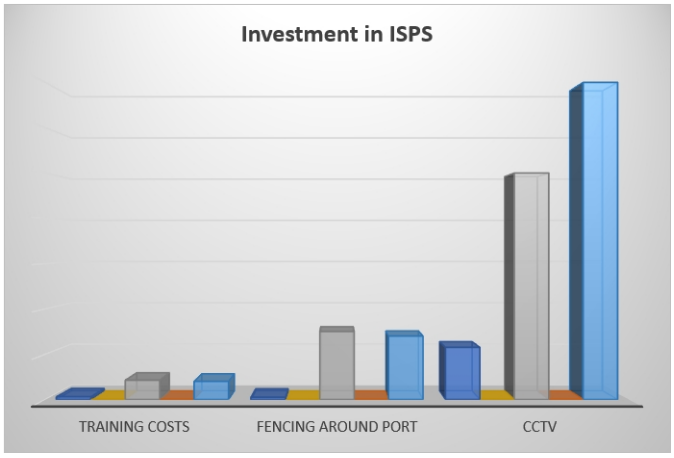
9. The present circumstance of Investments in ISPS.

The outline beneath delineates the things wherein the ports considered put resources into security up to the date of the examinations; it shows the three significant cost things for every port class. The expenses are communicated in US$. The expenses brought about by the Ports are a lot higher than the expenses acquired by the administrations or the port clients in referenced three port classifications the Port Authority caused almost every one of the expenses, yet is recuperating these from the port clients through a security charge. To be sure, none of the three governments spent noteworthy aggregates of cash to execute the ISPS Code. For the port clients, the expenses additionally were negligible, with the exception of the security charge that is required in Category Port A3.

The outer border fence of a project for a port falls under this category. The planned expenditures were about US $ 500,000. The fencing project was on the financial frontier for the next 1-2 years.

Pallet lighting for one of the ports of this category and through follow-up was expected to be completed within three years. The Port A3 seemed to have tremendous control at the end of its holder and the rest of the port gave the impression of good control, arrangement and demand. The general impression was that shipping security was high on the impulse of port management. Port A3 was also monitoring the CSI (Container Security Initiative) and the C-TPAT (Customs and Trade Partnership Against Terrorism Partnership) and did not prohibit the possibility of joining the CSI. From the point of view of a shipper, looking at the Port A3 class contains all the distinctive signs of having clear positive signals to deal with the original plan of the ISPS code - ensuring ships from unauthorized access and anonymous shipping - in the ideal way. On the other hand, ports under this category still face some significant difficulties in the fence and access control or implementation frameworks; it seems difficult for all intentions and purposes to monitor nearly 5,000 individuals, whenever they can be inside these ports. While each of the ports examined has been confirmed, it has not already reached a similar degree of security, due to variations in the scale and applicability of these measures. None of the ports put resources in freight scanners to control the payload. For example, one port has two scanners to control the import payload; a customs issue rather than a safety effort and the fact that port customers have been less concerned about the speculative restrictions so far in the preparation of ID cards.

Figure 3: Current conditions for investments in ISPS.



Source: Author.

Current conditions for investments in ISPS

The review below explains the things that ports take resources into account safely up to the date of inspection; it shows three cost-critical things for each port classification. Expenditures resulting from ports are considerably higher than those received by legislative bodies or port clients in three reference categories caused by the port authority, yet are recovered from port clients through security fees. Undoubtedly, none of the governments under this category have spent huge amounts of money to implement ISPS code. For port customers, expenses were similarly insignificant, except for the Port A3 class security fees.

10. Port security costs.

Overview, for each port, of investments related to ISPS and current (or operational) costs, as well as additional planned and required investments. From the totals, the annual and proportional costs related to ISPS were calculated. The various components of the annual investment costs have been achieved based on a number of variables:

- Investment costs,
- Percentage of investment costs attributable to ISPS, and
- Estimated investment life.

It should be noted that although the figures provided provide relatively similar results (completed and planned investments in order), this does not mean a completely similar situation at each port. By reviewing the status of ports that responded to safety and security checks. Ports under category A3 were the highest level, but still with some shortage. ISPS, or International Code of Ship and Port Security, is an essential perimeter guide for the safety and security of ships, ports, cargo and staff. Prior to the ISPS code, SOLAS's primary center was the well-being of the ship. Since security and well-being are completely different themes, new changes have been made in SOLAS and Chapter XI, which includes measures to improve

the level of oceanic well-being, by renaming to Chapter XI and Chapter XI included additional levels of safety in the middle of the sea. This new section contains guidance known as the International Ship and Port Facility Security Code (ISPS) with the restricted name "ISPS or ISPS Code". Since the ocean is probably the most effortless way to reach a global area, SOLAS's International Maritime Organization (IMO) displays Part XI-2 International Ship and Port Security Code - ISPS code for the welfare of ships and ports, sailors and government offices. The ISPS code was implemented by the International Maritime Organization (IMO) on July 1, 2004 as a comprehensive set of measurements of international security by assigning responsibilities to government authority, port authority, shipping companies and sailors. Applies to vessels on international flights, which include passenger ships and cargo ships of 500 GT and above. All things considered, everything began after the 9/11 assaults. The IMO (International Maritime Organization) understood that what occurred noticeable all around could likewise occur on the ocean or through the ocean. In this manner, the IMO chose to create, prescribe and actualize many safety efforts, relevant to boats and port offices around the globe. These measures named as the International Ship and Port Facility Security Code (ISPS). They are actualized through International Convention for the Safety of Life at Sea (SOLAS), 1974 section XI-2 to improve oceanic security.

11. The ISPS fees.

There are many stakeholders involved in enforcing and enforcing a safety code regardless of whether you are a shipper, exporter or merchant in the field of delivery and trade, you should know the key to understanding sea freight rates before entering the business. Mysterious, unexpected and unbudgeted delivery and shipping expenses may mean the end of activity for a number of parties, so they must be controlled and verified with interest. By examining your cargo transport locations or entering goods receipt structures, you may see charges called ISPS Charge, ISPS Surcharge, or ISPS only. This should not be considered just other delivery shortcuts that are generally loaded with truncation. This is something that is more profound than part of other related shipping charges. This will enable States that have participated in the Code to assess, recognize and survey the security risks to their ports and to take appropriate measures to determine the safety levels to be followed and compare security / preventive measures taken. To initiate certain functions and obligations, everything has been distributed to (governments and government offices that fall under this code, and to regulate ports, courier and port offices) that are concerned, both globally and locally, to ensure maritime security and to share / apply security-related data to ensure ship owners Adequate and coherent maritime safety efforts for their ships with respect to the ISPS code, shipping lines, ports and terminals shall appoint appropriate security officials / authorities on each vessel, in each port office and in any orderly transport to prepare and implement safety designs to be implemented. The ISPS code must be implemented in its complete structure to ensure security and assurance for all involved. For the transport line and port, it entails additional costs for the work of the qualified and well-prepared staff to carry out the safety efforts required by the code. There is a lot of manpower, arrangement, and gear that enters into the implementation of the ISPS code and to ensure the safety and security of the ship's group and port personnel. To take care of these costs, transport lines charge ISPS surcharges. Customer may incur additional ISPS charges such as carrier insurance fees as well as terminal insurance fees. The carrier also bears the insurance fees for the protection and expenses resulting from the implementation of the ISPS code. There is also a charge for terminal security where the port is charged for their expenses in implementing the ISPS code at the port / station. The ISPS service fee structure is usually part of the shipping quote and needs to be paid along with the goods. In this way, anyone who pays the goods (shipper or representative) will also pay the additional ISPS fee. The amount of ISPS charges is determined by the line that depends on the port where the portion of these costs changes. Recalling the ongoing risks of maritime theft, activities such as ISPS provide very compelling reasons for shipping, group and ship insurance. Despite the fact that this may include some significant shortcomings now, these long-term insurance activities are intended for everyone.

12. Cost of compliance with ISPS code.

In this section, costs related to ISPS code implementation and code implementation will be discussed. In addition to the very high security investment costs, there are many efforts that must be made to comply with the ISPS code. Costs include not only investments in materials (such as fences, control centers, camera security, etc.), but also in studies, security plans, additional management personnel, and security itself. Many of the data available from the ports will be addressed, recognizing the paucity of these data to analyze the safety rules related to the safety of ships and port facilities, but there is still no uniform legal source for funding security measures. In order to avoid distorting compatibility between ports and terminals, there are proposals from several organizations to finance port security, including those recommended by the Economic and Social Commission, the European Parliament and several EU Member States. Moreover, pressure groups from the public and private ports sector. This legal framework aims to prevent confusion and avoid distorting compatibility between ports and terminals.

This distortion may or may be caused by varying degrees of government subsidies in different countries. Only differences in liability with respect to the financing of security measures can cause this distortion. It is therefore essential to achieve a uniform and binding legal framework for all parties.

The information contained in this section is based on the UNCTAD "Cost of Compliance" report (UNCTAD) on 14 March 2007. But in the EU there was also a study on the costs of security measures and the possibility of establishing a European legal framework as already mentioned

It is clear from the results of the analysis one thing is certain, is the high cost of compliance with the rules of safety and

security, although different depending on the levels that have been adopted for most of these Asian ports. But to what extent costs are already high, they can only be assessed through a study based on specific criteria. To give an idea of high costs, UNCTAD conducted a study based on questionnaires sent to affected parties in the ISPS Code. The same questionnaire criteria were adhered to in the paper. Furthermore, it should be noted that the responses are based on port and government questionnaires (shipping sector not included, due to limited response). Data and response were available from most developed countries, and the following key conclusions were reached. It is clear that there is full compliance with the law to varying degrees, and there is a general obligation to compulsory part A in accordance with the guidance in Part B. Nevertheless, in many cases, there are also additional measures that have been adopted by the government or industry.

12.1. Cost of compliance.

In order to comply with the new security system, there are costs to be incurred.

First, initial costs, on average, equipment costs represent the largest share of expenditures followed by infrastructure expenditures. These initial costs range from US $ 3,000 to US $ 35,000,000.

Secondly the annual costs where the bulk of the costs go to the staff. These costs are estimated to be between $ 1,000 and $ 19,000,000.

Third, unit costs and rates are based on a few parameters including the annual revenue of the ports, the productivity of the goods, the number of port facilities according to ISPS requirements, and the frequency of the ship. Unit cost analysis shows a significant difference in small and large outlets, with smaller outlets having higher relative costs.

The initial port-related costs are estimated at between US $ 1.1 billion and US $ 2.3 billion. The annual amount is from US $ 0.4 to US $ 0.9 billion.

The equivalent of these costs in sea freight payments increases about 1% initially and 0.5% per annum of expenditure. With regard to the financing of some outlets, we can say that there are many responsive outlets that have already implemented cost recovery plans or are planning to implement them. It also turned out that it was still not possible to recover all costs, such as initial and annual financial costs.

It turned out that many ports had received funding and public assistance. In developed regions, assistance also involved the preparation of cost-sharing agreements and government grants. On the other hand, in developing countries, they can only benefit from technical assistance and capacity-building as directed by international organizations.

Moreover, it became known that despite a few exceptions, compliance with ISPS rules was reached without any difficulties by the respective national ports and the shipping sector. However, the majority of Governments indicated that additional measures have been implemented to comply with ISPS requirements. In terms of costs on behalf of governments, there is an initial cost of between $ 13,500 and $ 50 million per government. Annual costs are estimated at between US $ 1,500 and US $ 27 million. Despite cost recovery, most responding governments cannot recover this using user fees. However, governments prefer to recover their costs from certification and renewal fees as well as audits. In addition, some Governments wish to provide assistance to national ports through measures such as grants, cost-sharing arrangements, as well as technical assistance.

Some governments also noted that high implementation costs and the need for additional guidance are negative points for the new system to comply with code requirements. To the extent that it is already clear that most States are implementing additional measures to their regulations, the ISPS Code can be considered as a minimum security.

Moreover, it is necessary to set the costs right while adhering to the ISPS Code. We also point out the economic impact of applying ISPS code on various port measures such as efficiency, competitiveness, productivity, use of ICTs, reduced delays, theft and other criminal incidents.

Interestingly, average costs are higher in smaller ports than in larger ports. What also plays a role in the cost budget is the metric economy (for example below), the type and structure of the shipment, productivity, and the current security environment that existed before the implementation of the ISPS code. Therefore, the degree of security presence before the implementation of the code plays an important part, and the justification for this is that the smaller ports have a larger gap to fill than the larger ports where there was already more international traffic and already provided improved security. For example, we can point out that there is a large transit area where the acquired equipment is already owned and where measures have already been implemented that can be used for security purposes even though they were originally used for security or anti-theft requirements.

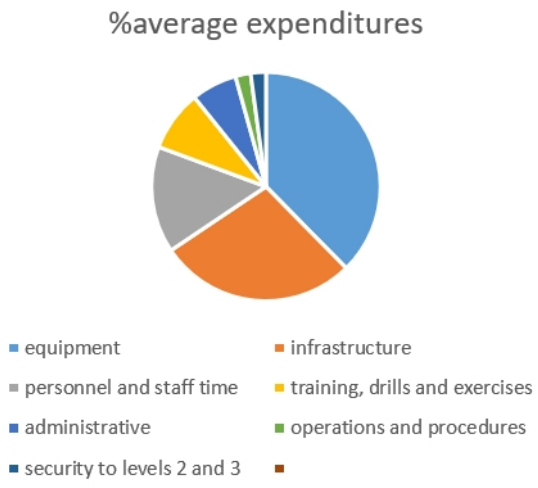
Regarding the factors that cause costs, there is a brief summary below. Initially there are initial costs:

This diagram clearly explains that the costs concerning the equipment are the largest cost factor for the ports (35%), followed by the expenses concerning the infrastructure (26%). These two factors are followed by the personnel costs(14%) who are involved in order to comply with the requirements of the ISPS Code and who need to fulfil to the training(8%) and the annual drills in addition to that.

It is also important to remark that with a transition to the security levels 2 and 3 there is an increased cost than when there is an operation on the regular level 1.

When looking further on to the factors of the costs on a yearly basis there a completely different conclusion has been come to:

Figure 4: Expenditures average %.



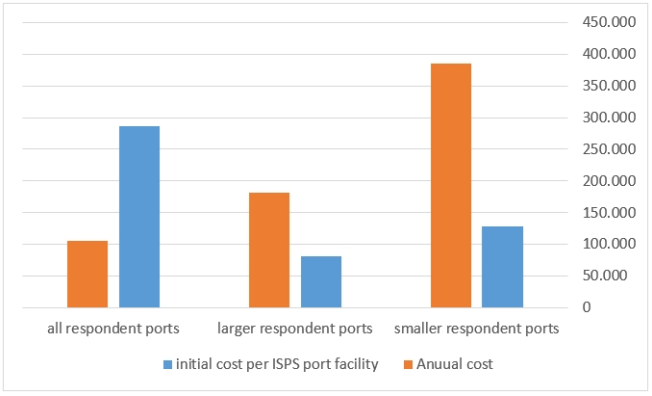
Source: Author.

The personnel costs with their 47% of the annual costs for the ports take the lead. These are followed by the training, the drills and exercises, which need to be pursued. Thus from this it can be deduced that the ISPS Code causes also an extra employment next to its costs.

13. The reflection cost of ISPS:

Initial cost and annual per ISPS facility.

Figure 5: Initial cost per ISPS.



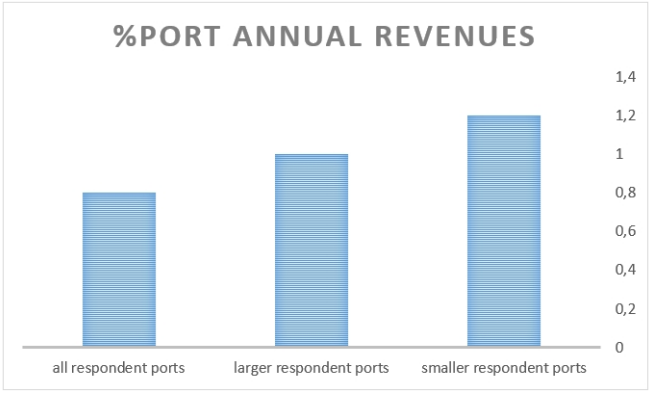
Source: Author.

Figure 2 above highlights the unit cost differentials that prevail between respondent ports depending on the number of ISPS port facilities with no further information on the type of traffic handled. The average initial cost per ISPS port facility for smaller respondent ports amounts to US$ 386,000 which is more than double the cost for larger respondent ports (US$ 181,000). The average initial cost per facility for all respondent ports, irrespective of the number of the ISPS port facilities, amounts to US$ 287,000. As to the annual costs, the average cost per facility for smaller respondent ports continues to be higher (US$ 128,000) as compared with the cost of larger respondent ports (US$ 81,000). The average annual cost per ISPS port facility for all respondent ports, irrespective of their size, amounts to US$ 105,000

14. Average Costs as a Percentage of Operating Revenues.

On average, the ISPS Code-related initial costs account for about 1% of respondent ports' annual revenues (Figure 3). A breakdown of respondent ports by size indicates that smaller respondent ports allocate a larger share of their operating revenues to financing the ISPS Code (1.2%) as compared with the share allocated by larger respondent ports (0.8%).

Figure 6: ISPS Code-related initial costs.

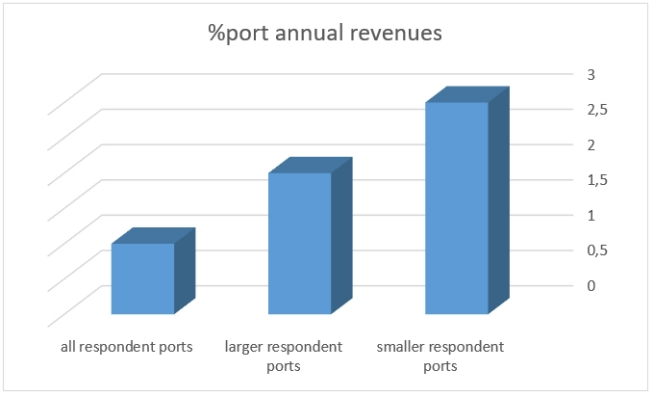


Source: Author.

- The relevant sample represents respondent ports handling about 8% of the global port cargo throughput (tons).
- Smaller ports up to 45 million $.
- Larger ports annual revenues over than 45 million $.
- All port (small and large port).

As to the ISPS Code-related annual running costs, on average, respondent ports allocate about 2% of their revenue to financing the ISPS Code-related expenditures (Figure 4). Smaller respondent ports allocate a larger share of their revenue (3%) to financing such costs as compared with larger respondent ports (1%).

Figure 7: ISPS Code-related annual costs.



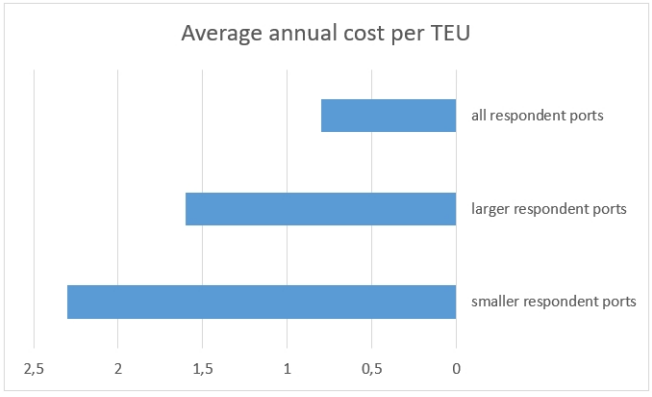
Source: Author.

The above results suggest that the ISPS Code-related financial impact is more pronounced in the case of smaller ports. Taking the analysis one stage further and accounting for other relevant parameters such as cargo throughput and ship calls, the following sections confirm the above findings and support the argument that cost differentials among respondent ports depend on size.

15. Average Costs per TEU Handled.

Taking into account the volume of container throughput handled, with no particular assumptions made with respect to the distribution of such traffic between respondent ports, the average cost per TEU for relevant respondent ports amounts to about US$ 1.6 (Figure 5). The average initial cost per TEU for smaller respondent ports amounts to US$ 2.3 about three times (US$ 0.8) the cost for larger respondent ports.

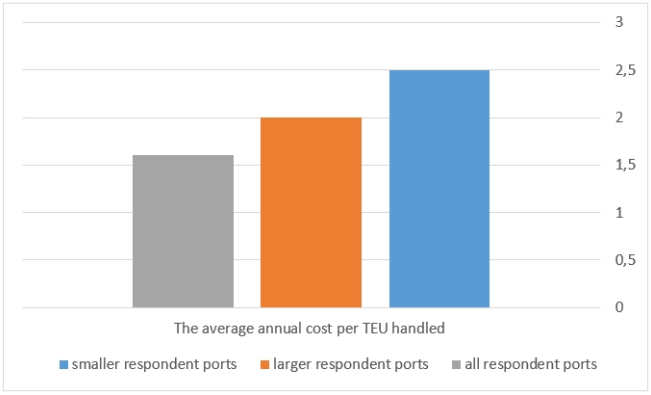
Figure 8: Average Costs per TEU Handled.



Source: Author.

A similar picture emerges when considering reported annual costs (Figure 6). The average annual cost per TEU handled for smaller respondent ports amounts to US$ 2.5, while the cost for larger respondent ports amounts to US$ 1.6. On average, the annual cost per TEU for respondent ports, irrespective of their size, amounts to US$ 2.

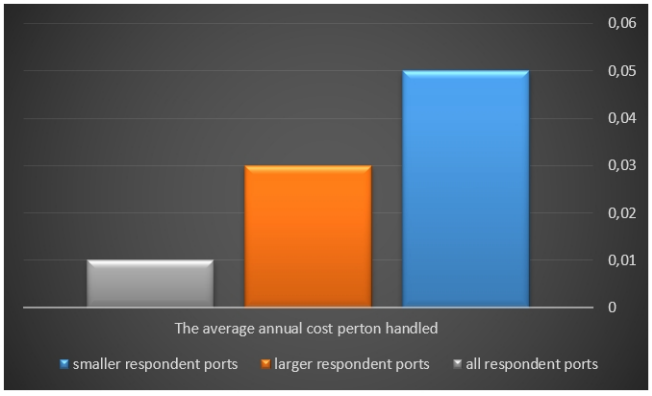
Figure 9: Average Costs per TEU Handled.



Source: Author.

Average Costs per Tone of all Cargo Handled 33. Using a different reference point tons of cargo throughput the average initial and annual unit costs have been assessed. The average initial cost per tone (Figure 7) for larger respondent ports amounts to approximately US$ 0.01, while that of smaller respondent ports is about US$ 0.05 or five times the average unit cost of larger respondent ports. The average initial cost for respondent ports irrespective of size amounts to US$ 0.03 per ton.

Figure 10: Average Costs per Ton Handled.



Source: Author.

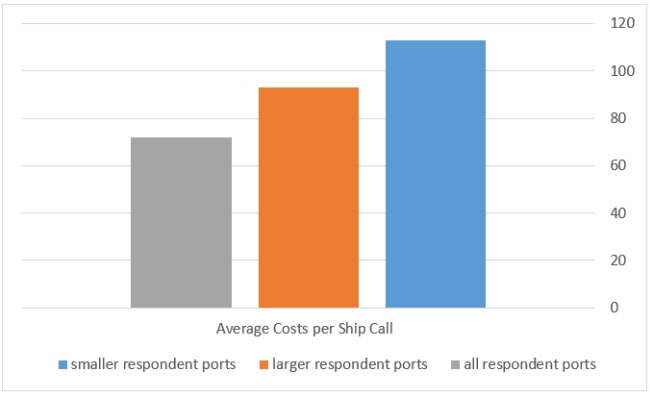
This result is replicated when considering annual costs (Figure 8). The average cost per tone for smaller respondent ports amounts to US$ 0.06 or double the average unit cost of larger respondent ports (US$ 0.03). The average annual cost per tone of cargo handled amounts to US$ 0.05 for all respondent ports irrespective of size.

16. Average Costs per Ship Call.

Figure 9 presents the results of an assessment of average unit costs based on the reported number of annual ship calls with no further information with respect to ship size, type and berthing time. Again, smaller respondent ports have an initial cost per ship that is higher (US$ 113 per ship call) than the cost of larger respondent ports (US$ 72 per ship call). The average

cost for relevant respondent ports, irrespective of the number of ship calls per year, amounts to US$ 93 per ship call.

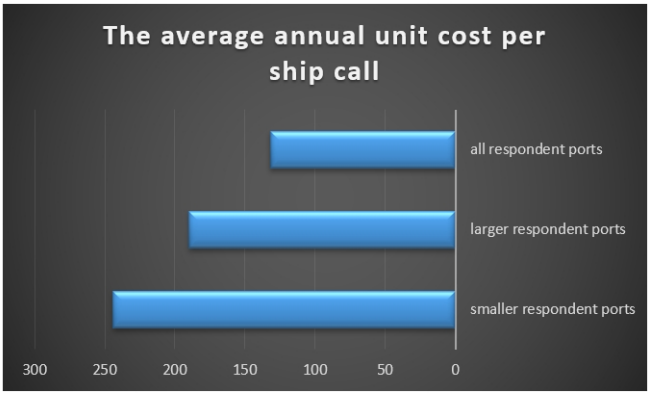
Figure 11: Average Costs per ship call.



Source: Author.

The average annual unit cost continues to be larger for smaller respondent ports (Figure 10) and amounts to US$ 244 per ship. The average cost per ship call for larger respondent ports and for all respondent ports irrespective of size amount to US$ 132 and US$ 190, respectively.

Figure 12: Average annual unit Costs per ship call.

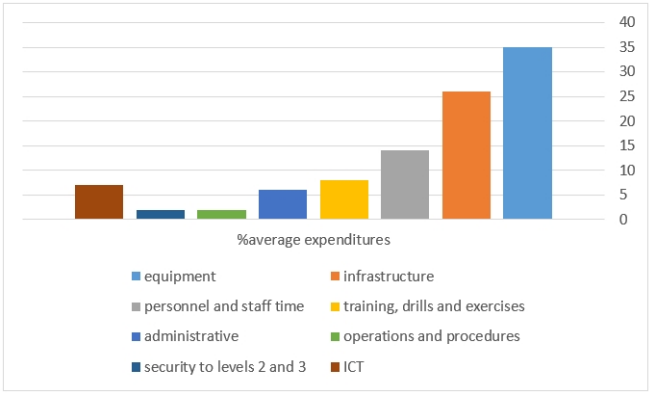


Source: Author.

17. Cost Factor Distribution.

As to the manner in which costs are distributed among various cost headings (Figure 11), responses received suggest that, on average, expenditures on equipment absorb the largest share of the initial costs (35%) followed by expenditures on infrastructure (26%). Other cost factors include expenditures related to personnel and staff time requirements (14%), training, drills and exercises (8%), ICT use (7%), administrative (6%), operations and procedures (2%) and upgrades19 of security to levels 2 and 3 (2%).

Figure 13: Average expenditures.



Source: Author.

18. Sources of financing the costs of implementing the code.

First of all, there are market-managed solutions, where port users are taxed for cost recovery and application expenses. The paper highlights the multiple possibilities for recovering the initial and annual costs associated with implementing the ISPS code. Find out whether they have already implemented the cost recovery schedule through port legislation, or if they plan to implement this type of recovery and the expected timeline. Which responsible parties should fulfill the implementation and clarify the basis of taxes. And projections for initial and annual cost recovery. From UNCTAD reports, the majority of outlets do not have a specific cost recovery schedule. However, but have the intention to introduce these tables. The report indicated that (6%) already provided these tables besides general support.

On the other hand, ports in developing regions, which have very limited use of cost recovery schedules, will face difficulties in taxing port users. Furthermore, it should be noted that some port operators are bound by their lease or concession agreement

As in the case of Jeddah Islamic Port (Red Sea Gateway - Dubai Ports), which causes the limitation of responsibility in determining the prices and collective revenues of port users.

It is becoming clear that ports generally prefer a tax approach in which many port users bear those costs, and there is even a tendency to tax goods.

There is also a preference (61%) of the ports included in the report for direct cost recovery from port users, and within about half of the initial costs related to ISPS Code. Other outlets (31%) expect cost recovery between 50% and 80%, and only a few (8%) expect full or almost full cost recovery.

Most outlets (54%) would like to recover more than half of their annual costs, but not necessarily the full amount. The other 46% of ports do not expect to recover more than half of the annual costs.

From these conclusions, it can be assumed that the expected level of recovery does not reach more than half. However, it is not clear how best to divide the refunds among many port shareholders.

The most important question with respect to cost recovery

schedules is whether port charges are commensurate with security costs and what are the merits?

In this regard we recommend the rule (cost out of the act), ie the amount of security service provided by the code is borne according to the levels of application, ie through the security services that have been strengthened**.**

19. Public or government funding.

The aim is to clarify the government or community role to finance the implementation of the Safety Code. About 26% of ports located in developing countries have been granted or expected to receive government support. Another part (6%) reported that they were not only given or were on their way to support, but also applied or were in the process of cost recovery schedules. It was also clear that all the ports (100%) that received or who were receiving government support were in public ownership. Many ports went to lay the foundations for cost sharing, while some of them were established A 75-25 cost-sharing agreement, to assist ports and port facilities in implementing the security measures contained in their security plans. Moreover, there can be interest-free loans, subsidies and tax credits.

With regard to sources of support, the main source of support for the majority of ports (82%) is local or national government. If other sources of support are regional organizations or interstate support. Along with support, technical assistance and capacity building are also forms of assistance

Conclusions.

Exchange of information between nations and ships should be promoted, but there must also be the possibility that in the event of armed robbery in the territorial sea, other States may cooperate or even take appropriate action when there is a risk of certain action being taken against other flag States. In addition, it should also be noted that insurances covering the interests of crewmembers in the event of such security breaches or armed robbery attacks should be due by IMO due to an increase in such breaches. ISPS has made it clear that there is a better information system to deal with these violations, and has imposed greater responsibility on flag states (for example, the security level system). When issuing these rules, it is important to create clear and effective rules, so that there is no discussion of different interpretations and the object is clear.

The implications of security measures are not few, and international trade now has less freedom because of strict control as well as because of providing detailed information to enhance security. It is not only the government that makes investments, but the private sector also needs to make investments. It becomes clear that the operating capacity of the transport sector has shrunk. However, I just wanted to draw attention to the fact that opinions are very divided, some say that the blog delays the supply chain tremendously, due to many formalities. Nevertheless, the application of security levels is nothing but protection for the assets of ships and ports and protect the foreign trade of the State and protection due to ensure the flow of global maritime trade. The Code has many advantages in the field of security and the Code makes the international transport sector safer and better. Obviously, there are still gaps in the rules here and there, and by working together and gathering regularly at conferences to assess what the ports have reached, the rules will become more modern and up-to-date. Moreover, it is also important to pay attention to the fact that the ISPS code can only provide security in its own domain. When action is taken against crimes against humanity, we need to seek a solution in other rules. We also recommend that the additional costs arising from implementation should be remedied. Levels of application of the safety code because it will eventually return positively to developed countries.

Acknowledgment.

The researcher expresses his thanks and appreciation to the DSR at King Abdul-Aziz University for its support to the research project no. D1435-90-980

References.

Convention for the Safety of Life at sea,(SOLAS 1974).

Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, updated and revised in 2005.

Convention on the Facilitation of Maritime Traffic, 1965.

International Ship & Port Facility Security Code(ISPS) 2002.

International Safety Management Code(ISM) 2002.

ALEXANDER Y.; RICHARDSON T.B., Terror on the high seas: from piracy to strategic challenge, California, Praeger Security International.

BIST D.S., *Safety and security at sea: a guide to safer voyages*, Oxford; Boston: Butterworth-Heinemann, 2000.

BRAGDON C.R., Transportation Security, Burlington, Butterworth-Heinemann Elsevier, 423.

CHALK P., *The maritime dimension of international security : terrorism, piracy, and challenges for the United States*, Santa Monica, 2008.

COOK A.T., *Managing global supply chains : compliance, security, and dealing with terrorism*, Auerbach; London, Taylor & Francis, 2008.

DE BACKER E., *Scheepvaartbeveiliging na 11 september: de mogelijkheden van de ISPS-code in Europa*, plaats, uitgever, 2004.

FRITELLI J.F., *Port and maritime security: background and issues*, New York : Novinka Books, 2003.

GUAN KWA C.; SKOGAN J.K., *Maritime Security in Southeast Asia*, Routledge, 2007.

HERBERT-BURNS R.; BATEMAN S.; LEHR P., *Lloyd's MIU handbook of maritime security*, Auerbach; London, Taylor & Francis.

ICS, *Model ship security plan : to assist shipping companies prepare ship security plans that comply with the IMO International Ship and Port Facility Security (ISPS) Code*, London, -International Chamber of Shipping.

ILO, *Security in ports: ILO and IMO code of practice*, Geneva: International Labour Office ; London: International Maritime Organization, 2004.

IMO, *Ship Security Officer*, London: International Maritime Organization (IMO), 2003.