Analysis of the Methodology Used for the Determination of Security Levels in the Port of Manta, Equator*

Análisis de la Metodología a Emplear en la Determinación del Nivel de Seguridad del Puerto de Manta-Ecuador

DOI: http://dx.doi.org/10.17981/ingecuc.11.2.2015.01

Research Article - Reception Date: March 1, 2015 - Acceptance Date: September 15, 2015

Mariela Jahaira Macías Párraga
Master in University Systems of Civil Engineering: Transportation and Territory, Universidad Politécnica de Madrid, Quito. (Equator). mj.macias@alumnos.upm.es , mmacias@mtop.gob.ec

María Nicoletta Gonzáles Cancelas
Doctor in Superior Technical Engineering of Roads, Canals and Ports, Universidad Politécnica de Madrid, Madrid. (Spain). nicoletta.upm@gmail.com, nicoletta.gcancelas@upm.es

Francisco Soler Flores
Doctor in Computing Engineering, Universidad Politécnica de Madrid, Madrid. (Spain). f.soler@upm.es

To reference this paper:
M. J. Macías Párraga, M. N. Gonzáles Cancelas and F. Soler Flores, "Analysis of the Methodology Used for the Determination of Security Levels in the Port of Manta, Equator," INGE CUC, vol. 11, no. 2, pp. 9-17, 2015. DOI: http://dx.doi.org/10.17981/ingecuc.11.2.2015.01

Abstract— This research aims to develop a methodology to evaluate the security of Manta Port progressively achieving secondary objectives that culminate in the creation of a risk matrix. A simple quantitative and qualitative methodology is used; it determines the combination of risk with the damage that could be caused, along with the estimated probability of an incident, thus, leading to a risk assessment. As a final result, a risk matrix for the Port of Manta was developed, which is the final chapter in the development of the suggested methodology; besides, it presents a clear and true picture of risk assessment so as to determine security levels and develop a method feasible to be implemented in any port of the world.

Keywords— Ports, Security, Risks, Protection Measure, Vulnerability, ISPS, SOLAS

Resumen—Este trabajo de investigación tiene como objetivo desarrollar una metodología de evaluación de la seguridad portuaria de Manta, alcanzando progresivamente objetivos secundarios que culminan con la creación de una matriz de riesgos. Se emplea una metodología sencilla, tanto cuantitativa como cualitativa, que determina la combinación del riesgo con el daño que se podría causar, junto con la probabilidad estimada de que ocurra un incidente, dando así lugar a una valoración del riesgo. Como resultado final se elaboró una matriz de riesgos del Puerto de Manta, siendo el acápite final del desarrollo de la metodología propuesta, además de que presenta un panorama claro y real de la evaluación de riesgos que permite determinar los niveles de seguridad; asimismo, desarrolla una metodología que puede ser implementada en cualquier puerto del mundo.

Palabras claves— Puertos, Seguridad, Riesgos, Medida de Protección, Vulnerabilidad, PBIP, SOLAS

* Research article derived from the research project: "Metodología DDSS de planificación portuaria. Aplicación al Puerto de Manta". Funded by the Universidad Politécnica de Madrid and Departamento de investigación de ingeniería e infraestructura del transporte. Starting date: 2013. Compleition date: 2016.

I. Introduction

Protection is an essential component in the economic feasibility for the sea transport system and international competitiveness [1]. It also should contribute towards the prevention of crime, terrorism, and other types of threats, like illicit trafficking of drugs, weapons, people, and other forms of organized crime, as well as other criminal offences that affect freight security and marine transportation (armed robbery, stowaways, contraband, among others) that constitute a hazard to trade, port activities, and shipping services [2].

Globally, terrorism is perceived as a permanent risk marked with constant occurrence likelihood of hostile actions; in this way, the International Ship and Port Facilities Security (ISPS) code adopted in the SOLAS Convention (December, 2002 in London) promotes this course of action [3], [4].

Facing the new international scenario, the General Administration of Ports in Equator established a specific area within every Port Authority to assume the responsibilities that derived in the new internationally agreed regulation in regard to security. The Department of Port Security was created especially for the operative implementation and application of the different international norms about security, counterterrorism, and environmental control, the ISPS code, for example [5].

Qualified personnel and the promotion of technology development are required for preventive control in the port jurisdiction, backing Manta's Port Authority decision on creating an administration specialized in comprehensive security matters.

Certainly, port security may arise as a relevant topic in international trading negotiations and government's orientations about the maritime field should be coordinated so as to ease the application of effective solutions.

Port authorities need to create the means to exchange updated information on port security matters and to disseminate prevention measures within the commercial sector [6].

The problem posed is treated with a research strategy that, with rigor, fulfills certain methodological parameters, this is, quantitative and qualitative methods but with a hybrid process (which, from diverse perspectives, is always beneficial). A methodological triangulation is always the result of blending and joining qualitative and quantitative strategies [7], as it will be explained in section III.

II. Literary Review

Since 9/11, a massive increase in personal, commercial, and governmental expenses in favor of counterterrorism strategies has been observed, just as the proliferation of programs for fighting terrorism [8], [9]. In 2002, the budget destined for counterterrorism and critical infrastructure protection was doubled [10] and, after issuing the HSPD 7 (Homeland Security Presidential Directive 7) in December 2003, which establishes a national policy for Federal Agencies and Departments whose aim is identifying, prioritizing, and protecting critical infrastructure, it was sixfold by 2004 [11].

However, this estimation does not represent the total amount of defense investment in the United States. Large quantities have been directed for the creation of government agencies like the Deparment of Homeland Security (DHS), the restructuring of the Department of Defense with the conformation of the Northern Command (*Northcom* which is in charge of the territory defense of countries like the U.S., Canada, Mexico, and part of the Caribbean), and the reordering of the Federal Bureau of Investigation (FBI) [12]; also for improving airport and border security, increasing research on response to biological or chemical agents, creating new laws, improving medical response for emergencies, providing help to other countries [13], and creating programs to reduce terrorism by strengthening potential objectives (e.g. reinforcing airport security control, placing barricades around buildings, or improving security for diplomats [14]).

Likewise, the Aviation and Transportation Security Act (ATSA) was enacted, in which the Transportation Security Administration was created for, as its name states, regulating public transportation in the United States [15]. It would also be responsible for the purchase, installation, and enhancement of monitoring equipment [16]; training security personnel; developing access protocols to control ramps, storage area, airplane parking spaces, and other restricted areas and facilities in cooperation with security managers in airports [17].

Specially, after 2004 Madrid train bombings, the European Commission (EC) wanted to improve security in different infrastructure types of the European Union considered as "critical", for this, a program with a course of action was put forward, including the creation of norms in order to support Member States identify them [18].

In 2004, the European Programme for Critical Infrastructure Protection (EPCIP) was created to help enterprises and public administrations of Member States complement and coordinate efforts in topics related to security and critical infrastructure identification, vulnerability, and interdependence, as well as for protection solutions and event preparation [19]. A national coordination body for CIP was created as the only supervision body of the EPCIP in the Member States [20].

There is also a large amount of literature available regarding risk analysis and security in maritime ports [21], as well as very specific and controlled protocols about this topic. Among the international regulations and treaties for security certifications are:

The *Safety of Life at Sea* or *SOLAS* treaty, the most important of all the international treaties about ship security. Its first version was approved in 1914 as a response to the Titanic catastrophe [22]. New versions have been adopted in 1929, 1948, 1960, and 1974, still in force. The treaty is subject of permanent amendments, whether by resolutions approved in the Maritime Safety Committee (MSC) meetings or by the International Maritime Organization (IMO) [23]. The main objective is to stipulate ship's construction, equipment, and usage norms so as to guarantee its safety and that of the people onboard.

The *ISPS code* is a new chapter within the SOLAS treaty that describes special measures to improve maritime security, explicitly, against terrorist or illegal actions; hence, it demands from ships, marine transportation companies, and port facilities the achievement of all the prescriptions established in the aforementioned code [24].

The *Container Security Initiative* (CSI) is a program implemented by the United States in January 2002 that represents an attempt of the Customs and Border Protection to substantially improve the detection of weapons of mass destruction transported by sea. It includes the presence of U.S. customs officers in foreign ports to identify and examine high risk containers, even before departing from their origin ports abroad, in order to prevent them from entering U.S. territory. Any suspicious container will be scanned and even unloaded by local port authorities before departing to the U.S. [25, 26]

The *Megaports Initiative* (2003) is a U.S. attempt for protecting the offshore grid from any hazardous cargo and nuclear materials. The aim is to scan, as much as possible, container trafficking regardless of their destinations and causing the least impact in port operations [27].

Other U.S. initiatives are the *Customs-Trade Partnership Against Terrorism* (CTPAT) whose objective is to extend as far as possible security perimeters to guarantee that importers transport their goods in secure associations since the moment the merchandise leaves the factory until the moment in which the retailer receives it [2, 28].

The *Business Alliance for Secure Commerce* (BASC) program, just as the Framework of standards to secure and facilitate global trade, aims at establishing global security standards and procedures to be implemented within the logistics chain of global trade. The implementation of this measure is not mandatory [29], [30] y [31].

The BTA or BioTerrorism Act, also known as the Public Health Security and Bioterrorism Preparedness and Response Act (PHSBPRA), is a norm based on the substantial amendments created by the Food and Drug Administration (FDA) statutes. This Act considers preventive criteria to counter bioterrorism actions by increasing control of food and biological elements flow [32].

The Authorized Economic Operator (AEO) is a program fostered by the World Customs Organization (WCO) that improves supply chain security, and also reduces cargo malicious handling and accident risks [33]; and the 24-hour rule, which forces maritime transporters to send detailed information of shipments 24 hours before stowing cargo for the U.S. [34].

U.S. initiatives will probably become global; however, they will translate into significant costs for ports of developing countries, for this reason, it is strongly recommended to be careful in its implementation.

The United Nations Conference on Trade and Development (UNCTAD)'s report on Container Security of February 2004, already warned about the higher costs and responsibilities these initiatives implied for these countries and the consequences these issues, besides port competition, might bring to small maritime terminals survival.

Within the most well-known security methods, the operational modality is evidenced in order to determine whether it is compatible with the set of security measures or not; in this way, in a public port, where free access for operation and stevedoring companies is the rule, is not suitable for the implementation of CSI, CTPAT, or BASC, since personnel control of multiple service providers cannot be ensured in the same manner as with an integral operator of a port terminal [35].

For a port terminal to be qualified for CSI, CTPAT, or BASC implementation, besides assuring operational management being provided by just one operator, it is also necessary exclusive access to the terminal and effective access control of vehicles, people, and merchandise, as well as its security management faculty [36].

In Equator's case, private entities that certify port facilities are

- Business Alliance for Secure Commerce - BASC
- Customs-Trade Partnership Against Terrorism-CTPAT

In the next section, a practical method for a worldwide application parallel to those established by the ISPS-BASC and ISPS-CTPAT will be suggested. This method is a user-friendly quantitative and qualitative valuation for each port to be implemented. For this case, the Department of Port Security of Manta can obtain its risk matrix so as to identify future and potential risks for every asset in the port.

III. Methodology

With the objective of developing an assessment methodology for the security in Manta's port, secondary objectives are achieved progressively in order to create a risk matrix, this means, a Port vs Security study [37].

The method applied for this study allows addressing port infrastructure security through clear guidelines and generating as result a risk matrix that includes aspects such as facilities and existing services; hazards like car bomb threats, illegal drug trade, stowaways, and ship hijacking; and the safeguarding equipment installed and detected vulnerabilities [38].

The stages for this method are summarized in Fig. 1:

Fig. 1. Methodological Process to Achieve the Risk Matrix of the Port of Manta. Source: Author

A. Previous Study of Infrastructure

First, a previous study of port infrastructures around the world needs to be performed so as to concentrate in the particular case later, this is, a top-down approach, from the general to the particular. According to the method proposed, transportation operation in the Port of manta is analyzed taking into account all its singularities as fishing, commercial, and passenger port [39].

Ports are comprised of different terminals, which in turn, are conformed of several subsystems, thus, complicating all the processes in the port. For this reason, a previous study of port facilities is required, which will be needed to determine the risk matrix or security matrix [40].

B. Threat Identification

Based on the history of attacks to ports and other transportation infrastructures, attacks most likely to happen against port infrastructure are identified, as well as the techniques and protocols to follow in such case.

C. Assets to protect

With public security and the strategic location in mind, a detailed analysis of the sea port is carried through with the aim of recognizing and classifying all the assets to protect.

All risks, vulnerabilities, and most importantly, the potential consequences need to be studied again in order to pose new methods, solutions, and safeguards against threats of high social impact [41].

D. Weaknesses

As of a detailed study, port infrastructure weaknesses are recognized, for instance, design, technology, operation, and management elements of assets that can increment the probability of a threat really happening. In the case of transportation infrastructure, passenger services prevail over secondary services offered in situ or in the vicinity [42]. It is important to remember that weaknesses, more if evident, may encourage threats to occur. Anyway, in all this chain, humans will still be the weakest link.

E. Existing Protection Measures

Closely related to weaknesses is the identification of existing protection measures. These can be attained from the infrastructure study during a field visit in which installed measures to date are collected, numbered, and described in detail [43].

A critical infrastructure may exhibit vulnerabilities regarding physical and sensible threats and not be able to consider safeguards of each type in separate plans. Likewise, all the safeguards must be integrated into a master plan because, currently, critical infrastructure operators have to follow many security plans: sectoral strategies, comprehensive security, safety of the operator, specific protection, emergency, business continuity, self-protection, industrial safety, etc. [44].

As multidisciplinary project, challenge-oriented policies and regulations are to be posed towards the demands of each milieu, differentiating the necessities of the government, the industry, and the users [45],[46].

F. Risk and Consequence Analysis

Currently, as stated before, critical infrastructure operators, like sea ports, have to follow many security plans, hence, security convergence is strongly recommended [47].

The next step is estimating attack occurrence probability and its impact provided it actually happened. For this, a hazard analysis for the infrastructure's most relevant assets is performed together with a quantitative valuation of a given

threat's risk and its possible aftermaths [48]. First, the likelihood of occurrence of a threat event is assigned, and afterwards, the impact it could have is also defined. In this way, the risk level will be mapped for every asset in regard to the threats considered.

To determine the likelihood of a hazardous event, a qualitative estimation is carried through using a scale which goes from highly unlikely to very likely, as seen in Fig. 2. Likewise, the impact produce in case of a real event can also be classified; this varies in a scale from low to very high.

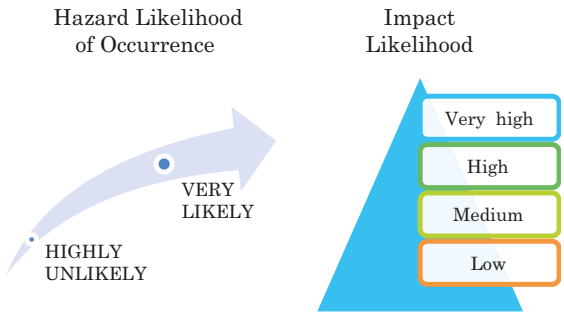

Fig. 2. Likelihood of Occurrence: Hazard and Impact. Source: Author

Table I illustrates the result of crossing the impact and hazard likelihood values (impact * hazard likelihood); in Table IV, the assignation of number values for each situation is shown.

Table I. Impact vs Hazard Likelihood

IMPACT	HAZARD LIKELIHOOD OF OCCURENCE				
		Highly Unlikely	→		Very Likely
	Very High				
	↑				
	Low				

Source: Author

Finally, risk level classification is explained in Fig. 3. These levels are provided according to the valuation obtained in Table I and will belong to one category of this scale; it varies from low values, considered as *Risk 4* (Low), to high values, classified as *Risk 1* (High).

Fig. 3. Risk Levels. Source: Author

This last valuation of risk levels can be associated to colors so as to facilitate risk matrix interpretation, thus, Risk 1 will be colored as red, Risk 2 as orange, Risk 3 as yellow, and Risk 4 as blue. This is a very fast and intuitive manner of indicating risk levels in the scenarios analyzed.

G. Risk Matrix

Ultimately, the process of port security planning should allow elaborating and implementing measures for port vulnerability reduction [49]. If this possibility is not recognized, countermeasures cannot be elaborated. Port security administration should be in conditions to determine the nature and magnitude of any hazardous event affecting the security of the operations [50]. As a consequence, the first task in the process of a security regime establishment in ports is to conduct a comprehensive analysis of security conditions [6].

With the data gathered in the previous stages, a risk matrix is elaborated for the Port of Manta. In this matrix, assets, along with the likelihood of occurrence of any hazard and the damages caused, provided the event actually happens, are displayed.

The final result will show the risk level associated to its corresponding color, in this manner, the analysis passes from an approximate qualitative estimation to a final quantitative valuation, which is more objective. Hence, port infrastructure elements are already classified with the risks each one poses.

IV. Results and Discussion

Once the methodology has been explained, results from the development of the method suggested are gathered in this section. In the next paragraphs, these results are described in detailed.

A. Previous Study of Infrastructure

A previous study of the infrastructure in the Port of Manta has been accomplished during the technical visit in 2014. It was used to determine the risk matrix.

As it was observed, the infrastructure of the Port of Manta is in optimum conditions after receiving a state contribution to rebuild the International Dock 1 and the Fishing Dock, replace the old pilings, and repair slabs from the berth line [51].

B. Threat Identification

From the threat identification through history incidents, it was concluded that threats against the port systems can be summarized in Table II, where the kind of hazard is also presented. The last hazardous events in the Port of Manta can be comprised in four large groups.

Table II. Port System Threats

Main Threats in the Port System			
Car bomb	Illegal drug trade	Stowaways	Ship hijack

Source: Author

C. Assets to Protect

Regarding public security and strategic location, a detailed study of the sea port is performed in order to recognize and classify all the assets to be protected, as shown in Fig. 4.

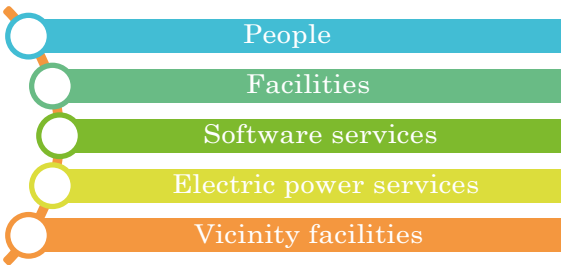

Fig. 4. Assets to Protect in the Port of Manta.
Source: Author

The approach to asset analysis can be performed in different ways. In the case of a sea port is easier to consider separately merchandise subsystems of solids, liquid, common goods, passenger terminal, etc., and subsequently, study each one of these typologies.

D. Weaknesses

As a consequence of the threat typification present in the Port of Manta, in this section all port infrastructure shortcomings are identified; this is, design, technology, operational, and management elements of assets likely to be hazard targets are recognized.

Once again, weaknesses, more when evident, can encourage threats to become real attacks.

The flaws detected in the Port of Manta revolve around IT systems used to identify abnormalities in the performance of port activities

E. Existing Protection Measures

Quite related to weaknesses is the identification of existing protection procedures. All measures aimed at detecting and/or decreasing threats are listed (e.g. access control, restricted areas, barriers, CCTV, etc.) and every port facility undergoes a checking procedure (Table III).

Exisitng protection measures in the Port of Manta are listed above. And to continue with the method's application, the next section analyzes risks and consequences, provided hazards or attacks become real in the port facilities [52].

Table III. Existing Protection Measures in the Port of Manta

List of Security Measures	Port of Manta – Equator
Access control barriers (Closing systems)	3 barriers
Entrance systems (barriers, huts)	2 people
People identification sytems	Yes
Peopleand vehicle search and tracking	Yes
CCTV (Closed Circuit TV)	Yes
Intruder detection	Yes
Fire and smoke detectors	Yes
Emergency and first aid equipment	Yes
Back-up systems	Yes
Communication systems	Yes
Personnel training	Yes
Emergency and evacuation procedures	Yes
Colaboration agreements	Yes
Security plan	Yes
Contingency plan	Yes
Dogs and patrols	Yes
Security guards	Yes

Source: Author

F. Risk and Aftermath Analysis

The result of the suggested method applied and described in prior sections is a table that estimates threat or attack likelihood and their impact. Results are both quantitative (valuation with numbers of hazard threats) and qualitative (risk allocation by colors).

Table IV allocates, first, the likelihood of occurrence of hazard threats, and second, the subsequent impact; in this way, risk levels are mapped for every asset before all threats.

Likelihood of occurrence was estimated in a qualitative manner with a scale ranging from *highly unlikely* to *very likely*. Likewise, to classify impact levels, a scale ranging from *low* to *very high* was adopted.

As final step, Table IV crosses impact and likelihood values and numeric values were allotted according to each situation. And finally, risk level classification is also presented: the lowest values, considered as Risk 4 (low), are green; and the highest values, Risk 1 (very high), are red. Intermediate values are also differentiated with yellow and orange.

Table IV. Impact vs Likelihood of Occurrence in the Port of Manta

Impact – severity levels	Likelihood of occurrence				
	(5) Very Likely	(4) Likely	(3) Sporadic	(2) Unlikely	(1) Very Unlikely
IV (Very High)	20	16	12	8	4
III	15	12	9	6	3
II	10	8	6	4	2
I (None)	5	4	3	2	1

Source: Author

G. Risk Matrix

In the application of this method, a risk matrix for the Port of Manta was elaborated as final outcome. The matrix sets forth the assets to be protected and the likelihood of hazard occurrence, also, the corresponding damage for the worst scenario: an attack event.

Table V poses risk levels associated to the corresponding color, as explained above. Hence, a more objective perspective with a qualitative and quantitative valuation can be observed. Every port infrastructure element was classified with the risks they present individually.

Table V. Risk Matrix for the Port of Manta

PORT OF MANTA		Car bomb	Illegal drug trade	Stowaways	Ship hijacking
ASSETS		**THREAT**			
People	Staff of Manta's Port Authority	3/IV	3/III	2/III	
	Cruise tourists			3/III	4/IV
	Merchant marine staff	1/III	2/III	3/III	4/IV
	Fishermen	2/IV	4/IV		5/III
	Longshoremen	2/IV	1/IV	1/II	2/III
Maritime Area	Mouth of the port	1/III	3/III	2/III	4/IV
	Water mirror		5/III	3/IV	4/IV
	Beaches	2/III	3/III	5/IV	
	Buoys and navigation aids		2/III	1/III	
Port Facilities	Inland port infrastructures	2/III	4/IV	3/III	
	Docks	2/III	4/III	2/III	4/IV
	Marine station	4/IV	4/IV	4/IV	
	Lighthouses	2/IV	1/II	2/III	
	Sea walls	3/III	4/III	3/III	4/III
	Yacht club	4/IV	3/III	1/III	4/III
	Truck parking lots	4/III	2/III	1/IV	
	Cranes and handling equipment	2/III	1/III	1/III	
	Maritime service stations (gas)	2/IV	2/III	4/III	
Other Important Facilities	Airport	4/III	3/IV	1/I	
	Petroecuador- Hydrocarbons	4/IV	2/II		
	Electrical power station	4/IV	2/II		
Software, Phones, and Power Lines	Database system and pone facilities	3/IV	3/III	3/II	
	Electrical installations	3/IV	1/I	1/I	
Ships	Fishing ships		4/IV	3/III	4/IV
	Passenger merchant vessels	2/IV	2/III	2/IV	4/IV
	Goods merchant vessels	2/IV	4/IV	3/IV	4/IV

Source: Author

The risk matrix was elaborated using benchmarking information and the data provided by the port authority of Manta during the *in situ* visit. Research criteria were added to estimate quantitative and qualitative valuations of risk levels for each asset under the circumstances previously mentioned.

V. Conclusions

The *Risk Matrix of the Port of Manta* was elaborated, it being the final stage of the method suggested in this paper. This matrix sets forth a clear and real perspective for risk assessment so as to determine security levels.

When analyzing the Risk Matrix of the Port of Manta, it is evidenced that the most exposed assets to hazard events are: *People*, fishermen; *Maritime area*, mirror of water; *Port facilities*, fishing ships and vessels; and the most probable hazards are *ship hijacking* and *illegal drug trade*. Thus, the port authority of Manta needs to concentrate efforts in them and create protection measures.

The information provided in this paper constitutes one of the most relevant contributions for the development of a method that can be implemented in any port of the world. It provides a user-friendly, quantitative-qualitative approach that allowed creating a risk matrix for every scenario, revealing existing critical assets and their valuation regarding the risks considered. Additionally, it can enhance the design and implementation of a comprehensive port planning method.

To conclude, the general objective of developing a risk assessment method that identifies security levels and systems to be improved was accomplished; in this way, it can be proved that this method is useful to, ultimately, provide more security to the Port of Manta and solve the problem posed in this paper.

References

[1] J. S. Helmick, "Port and maritime security: A research perspective," *J. Transp. Secur.*, vol. 1, no. 1, pp. 15–28, Dec. 2007. DOI: 10.1007/s12198-007-0007-3

[2] M. Sgut, *Efectos económicos de las nuevas medidas de protección marítima y portuaria*. Canada: Comisión Económica para América Latina y el Caribe, 2006.

[3] C. B. Acevedo, "El Código Internacional Para La Protección De Los Buques E Instalaciones Portuarias (Código Pbip). Orígenes Del Código Pbip," *Rev. Derecho La Pontif. Univ. Católica Valparaíso*, Vol. 25, Pp. 33 – 48, 2004.

[4] Ministerio de Asuntos Exteriores y de Cooperación, "Código Internacional para la protección de los buques y de las instalaciones portuarias (Código PBIP)," 2002. [Online]. Available: https://www.boe.es/buscar/doc.php?id=BOE-A-2004-15290..

[5] F. E. Hernández Custode, "Elaboración del sistema de gestión de prevención de riesgos laborales del Puerto de Manta," M.S thesis, Dept. Ind. Eng., Univ. Laica Eloy Alfaro De Manabi, Manta, Ecuador 2010.

[6] Comunidad Andina, "Seguridad portuaria: La Guía de Planificación Nacional," 2000.

[7] E. A. López, "Estrategias de Investigación," En Politica Fiscal y Estrategia como Factor de Desarrollo de la Mediana Empresa Comercial Sinaloense. Un Estudio de Caso, Culiacán, 2015.

[8] C. Macilwain, "Bush goes to war as budget boosts R&D.," *Nature*, vol. 415, no. 6872, p. 564, Feb. 2002. DOI: 10.1038/415564a

[9] J. Dawson and P. Guinnessy, "Terrorism drives bush R&D money to defense and NIH; Other science funding flat in fiscal 2003," *Phys. Today*, vol. 55, no. 4, pp. 30–36, Apr. 2002. DOI: 10.1063/1.1480779

[10] "The Budget and Economic Outlook: Fiscal Years 2003-2012 | Congressional Budget Office." [Online]. Available: https://www.cbo.gov/publication/13504. [Retrieved: 16-Sep-2015].

[11] "Testimony on The Budget and Economic Outlook: Fiscal Years 2006 to 2015Congressional Budget Office." [Online]. Available: https://www.cbo.gov/publication/16226. [Accessed: 16-Sep-2015].

[12] R. B. Manaut and C. R. Ulloa, "Seguridad y fronteras en Norteamérica. Del TLCAN a la ASPAN," *Front. Norte*, vol. 18, no. 35, pp. 7–28, 2006.

[13] C. Lum, L. W. Kennedy, and A. Sherley, "Are counter-terrorism strategies effective? The results of the Campbell systematic review on counter-terrorism evaluation research," *J. Exp. Criminol.*, vol. 2, no. 4, pp. 489–516, Dec. 2006. DOI: 10.1007/s11292-006-9020-y

[14] C. Lum, L. W. Kennedy, and A. Sherley, "Is counter-terrorism policy evidence-based? What works, what harms, and what is unknown.," *Psicothema*, vol. 20, no. 1, pp. 35–42, Feb. 2008.

[15] J. Hainmuller and J. M. Lemnitzer, "Why do Europeans fly safer? The politics of airport security in Europe and the US," *Terror. Polit. Violence*, vol. 15, no. 4, pp. 1–36, 2003. DOI: 10.1080=09546550390449863

[16] K. B. Lee and M. E. Reichardt, "Open standards for homeland security sensor networks," *IEEE Instrum. Meas. Mag.*, vol. 8, no. 5, pp. 14–21, Dec. 2005. DOI: 10.1109/MIM.2005.1578613

[17] R. W. Poole Jr And G. Passantino, A Risk-Based Airport Security Policy. 2003, Pp. 1–33.

[18] S. E. Flynn, "Port Security Is Still a House of Cards," *East. Econ. Rev.*, vol. 169, no. 1, pp. 5–11, 2006.

[19] T. G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. NJ: John Wiley & Sons, Inc., 2006. DOI: 10.1007/s12198-007-0007-3

[20] J. P. Burgess, "Social values and material threat: the European Programme for Critical Infrastructure Protection," *Int. J. Crit. Infrastructures*, vol. 3, no. 3, pp. 471–487, 2007. DOI: 10.1504/IJCIS.2007.014121

[21] P. Chalk, "The Maritime Dimension of International Security," RAND Corporation, 2008.

[22] H. Hesse, "Maritime Security in a Multilateral Context: IMO Activities to Enhance Maritime Security," *Int. J. Mar. Coast. Law*, vol. 18, no. 3, pp. 327–340, Sep. 2003. DOI: 10.1163/092735203770223567

[23] R. G. Bernal, M. Manosalva, S. Rezende, M. Sgut, and R. Sanchez, "Protección marítima y portuaria en América del Sur. Implementación de las medidas y estimación de gastos." pp. 7–61, 2004.

[24] A. Mazaheri and D. Ekwall, "Impacts of the ISPS code on port activities: a case study on Swedish ports," *World Rev. Intermodal Transp. Res.*, vol. 2, no. 4, pp. 326–342, 2009. DOI: 10.1504/WRITR.2009.026211

[25] K. Bichou and R. Talas, "Overview of contemporary supply chain security initiatives," in *Maritime Transport Security*, pp. 24–39. DOI: 10.4337/9781781954973

[26] S.Y. Yi, "'An approach to improve international maritime security through the coordination between the IMO instruments and the Proliferation Security Initiative (PSI) regime," M.S thesis, DeptMarit and Env.Admon. World Maritime Univ. Malmö, Suecia, 2013.

EDUCOSTA

[27] P. A. Elizalde Monteagudo, "La Incidencia de las Normas de Protección Marítima en el Transporte Marítimo," M.S thesis, Dept, Dret Privat. Univ. Autònoma de Barcelona, Barcelona, España, 2012.

[28] W. Keefer, "Container Port Security: A Layered Defense Strategy to Protect the Homeland and the International Supply Chain," *Campbell Law Review*, vol. 30, no. 1. 2007.

[29] P. Knight, '"Supply chain security guidelines," IBM, White paper, 2003. [Online]. Available: http://www-03.ibm.com/procurement/proweb.nsf/objectdocswebview/filesupply+chain+security+guidelines/$file/supply+chain+security+guidelines+12sep03.pdf

[30] F. Piniella, J. Walliser, and A. Martínez, "Global Maritime Security: the role of Spain as a Port State," *Journal of Maritime Research*, vol. 5, no. 3. pp. 15–32, 24-Jan-2014.

[31] K. Christopher, *Port Security Management*. New York: CRC Press Book, 2009.

[32] Center for Food Safety and Applied Nutrition, *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (PL107-188). United States: Center for Food Safety and Applied Nutrition, 2002.

[33] L. Urciuoli and D. Ekwall, "Possible impacts of supply chain security on efficiency - A survey study about the possible impacts of AEO security certifications on supply chain efficiency," Jun. 2012.

[34] Y.-C. Yang, "Risk management of Taiwan's maritime supply chain security," *Saf. Sci.*, vol. 49, no. 3, pp. 382–393, Mar. 2011. DOI: 10.1016/j.ssci.2010.09.019

[35] C. A. Vallejo Ramirez, "Drug transport in containers: Risk of international supply chain logistics," M.S. thesis, Dept. Rel. Internal. Estr. and Segur. Univ.Militar Nueva Granada, Medellin, Colombia, 2015.

[36] E. Sadovaya and V.V. Thai, "Maritime Security Requirements for Shipping Companies and Ports: Implementation, Importance and Effectiveness," 2007. [Online]. Available: http://www.icms.polyu.edu.hk/ifspa2012/Papers/M05.pdf

[37] M.M. Párraga, N. González-Cancelas and F. Soler-Flores, '"Port security applied to Transfer Port of Manta," *Advanced Research in Scientific Areas* pp.508-512, Dec. 2013.

[38] Cámara Marítima y Portuaria de Chile, "Normas Internacionales de Seguridad Antiterrorista: Su efecto en los Puertos Chilenos," 2014 [Online]. Available: http://www.cursos.ucv.cl/tra34500/pg000.html

[39] M. Autoridad Portuaria, "Puerto de Manta," 21 de Junio 2013, pp. 10.

[40] F. Soler-Flores, "Proposal for the integration of the Port of Manta in Latin American multimodal logistics," *Proc. GV - Glob. Virtual Conf.*, no. 1, Apr. 2013.

[41] "Using portfolio optimisation to calculate the efficient relationship between maritime port security residual risk and security investment," *Int. J. Shipp. Transp. Logist.IJSTL*, vol. 6, no. 3, pp. 314–338, 2014. DOI: 10.1504/IJSTL.2014.060788

[42] R. Núñez-Sánchez, S. Jara-Díaz, and P. Coto-Millán, "Public regulation and passengers importance in port infrastructure costs," *Transp. Res. Part A Policy Pract.*, vol. 45, no. 7, pp. 653–666, Aug. 2011. DOI: 10.1016/j.tra.2011.04.012

[43] R. Núñez-Sánchez, S. Jara-Díaz, and P. Coto-Millán, "Public regulation and passengers importance in port infrastructure costs," *Transp. Res. Part A Policy Pract.*, vol. 45, no. 7, pp. 653–666, Aug. 2011. DOI: 10.1016/j.tra.2011.04.012

[44] S.F. Aguas Almeida and L.E. Cevallos Karolys, "Modelo de desarrollo y aplicación del cuadro de mando integral en operadoras portuarias, caso Puerto de Manta," M.S thesis, Dept. Fin Eng., Univ. Central Del Ecuador, Quito, Ecuador, 2012.

[45] K. Bichou, J. S. Szyliowicz, and L. Zamparini, *Maritime Transport Security: Issues, Challenges and National Policies*, 1st ed., vol. 1. Massachuesetts, 2013.

[46] O. Doerr, *Politicas Portuarias*. Santiago de Chile: Naciones Unidas, 2011.

[47] M. McNicholas, "Guía Estratégica para la Seguridad Portuaria de Clase Mundial," 2011. [Online]. Available: http://www.phoenixgrouppanama.com/downloads/pdf/Port%20Security%20Primer_spn_.June%2002.pdf

[48] K. Bichou, M. Bell, and A. Evans, *Risk Management in Port Operations, Logistics and Supply Chain Security*, 2nd ed. New York: McGrawHill, 2014.

[49] C. Ducruet, '"The polarization of global container flows by interoceanic canals: geographic coverage and network vulnerability," *Marit. Policy Manag.*, pp. 1–19, Mar. 2015. DOI: 10.1080/03088839.2015.1022612

[50] C.A. Bernal Torres, '"Seguridad portuaria: una necesidad o una ventaja competitiva para Colombia," 2014.

[51] Ministerio de Transporte y Obras Públicas, Ecuador, "Plan Estratégico de Movilidad: Puerto de Transferencia de Manta,". [Online]. Available: http://www.puertodemanta.gob.ec/wp-content/uploads/2013/11/10-Plan-Desarrollo-Puerto-de-Manta.pdf

[52] Organización Marítima Internacional, "Protección en los puertos. Repertorio de recomendaciones prácticas," 2004. [Online]. Available: http://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/normativeinstrument/wcms_162330.pdf