Building a national maritime security policy

Adriana Avila-Zúñiga Nordfjeld

Follow this and additional works at: https://commons.wmu.se/phd_dissertations

Part of the Defense and Security Studies Commons, Emergency and Disaster Management Commons, Infrastructure Commons, and the Transportation Commons

This Thesis is brought to you courtesy of Maritime Commons. Open Access items may be downloaded for non-commercial, fair use academic purposes. No items may be hosted on another server or web site without express written permission from the World Maritime University. For more information, please contact library@wmu.se.
BUILDING A NATIONAL MARITIME SECURITY POLICY

by

ADRIANA AVILA-ZÚÑIGA NORDFJELD

WMU RESEARCH REPORT SERIES
No. 11, September 2018
Building a national maritime security policy
The aim of the WMU Research Report Series is to publish essays, monographs, articles, policy papers, occasional papers, reports, and PhD dissertations to promote academic research and publication among resident colleagues at the World Maritime University as well as other scholars associated with it. Publications in this series will be published in moderately priced limited offset editions.

Short excerpts from this publication may be reproduced without authorization, on condition that the source is indicated. For rights of reproduction or translation, application should be made to –

The Editors, WMU Research Report Series
World Maritime University
P.O. Box 500
201 24 Malmö
Sweden
Building a National Maritime Security Policy
Lessons from Mexico

Adriana Avila-Zúñiga Nordfjeld
Norway/Mexico

A dissertation submitted to the World Maritime University in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Maritime Affairs

WMU RESEARCH REPORT SERIES
No. 11, September 2018
WMU Publications
Cover photo by Adriana Avila-Zúñiga-Nordfjeld

Copyright pp. 1-134 Avila-Zúñiga-Nordfjeld, A.

Paper 1 © TransNav, Faculty of Navigation, Gdynia Maritime University, Poland

Paper 2 © TransNav, Faculty of Navigation, Gdynia Maritime University, Poland

Paper 3 © Gomylex Editorial

Paper 4 © Springer International Publishing

Paper 5 © World Maritime University

The views expressed are those of the author(s) and do not necessarily reflect the view or policy of his/her/their employer(s,) organization(s), WMU Publications, or the World Maritime University. WMU Publications and the Series Editors, while exercising the greatest care in this publication, do not hold themselves responsible for the consequences arising from any inaccuracies therein.

All rights reserved. Except for quotation of short passages for the purposes of criticism and review, no part of this publication may be reproduced without full attribution to the author(s) or the prior written permission of the Publisher.

ISBN: 978-91-984226-8-9

Published in Sweden in 2018
Printed by Media-Tryck, Lund, Lund University 2018

WMU PUBLICATIONS
PO Box 500
201 24 Malmö, Sweden

Suggested Citation:

Dedicated to Sebastian, my most precious companion sailing this doctoral journey
# Table of Contents

Acknowledgement ........................................................................................ 11  
Abstract ........................................................................................................ 13  
Abbreviations ............................................................................................... 15  
List of figures ............................................................................................... 17  
List of Tables ............................................................................................... 17  
List of papers included in this dissertation ................................................... 18  
Other works by the respondent..................................................................... 23

1. Introduction ........................................................................................................ 25

2. Frames of reference ............................................................................................ 31  
   2.1 International legislation for port and maritime security ....................... 31  
      2.1.1 The International Ship and Port Facility Security Code (ISPS Code) ................................................................................. 33  
      2.1.2 International Convention on Standards of Training, Certification and Watch keeping for Seafarers, 1978.......................... 37  
      2.1.4 United Nations Convention on the Law of the Sea (UNCLOS) & Port State Control......................................................... 38  
   2.2 National legislation in Mexico for port and maritime security .......... 41  
      2.2.1 Evolution of the maritime realm in Mexico ............................... 41  
      2.2.2 Port & maritime security legislation in Mexico ......................... 42  
      2.2.3 The maritime reform of 2017 that transferred Harbour Masters from SCT to SEMAR ............................................................... 46  
      2.2.4 The decree about safety & security zones for navigation and over flight in the surroundings of offshore installations........................................ 54  
   2.3 Current security threats at Mexican ports............................................. 56  
      2.3.1 Security threats related to port oil terminals ............................... 56  
      2.3.2 Criminal acts in relation to oil platforms located in the continental shelf................................................................. 61  
      2.3.3 Security threats related to ports and port facilities in general..... 66
2.4 The value of incident reporting and updating of PSA/PFSA & PSP/PFSP ................................................................. 67
2.5 Summary .......................................................................................................................... 68

3. Research objectives .................................................................................................. 71
3.1 General research objectives ...................................................................................... 72
   3.1.1 Elaborate a critical analysis of the current port security situation of Mexico, with special focus on implementation and compliance of the ISPS Code, including the state of the art and harmonization of international legislation with national law. ............. 73
   3.1.2 Identify the most relevant security threats to port facilities in Mexico, including oil terminals, and offshore installations .................. 73
   3.1.3 Develop an analytical instrument for security incidents-reporting & incident investigation, to strengthen the continual evolution of PSA/PFSA and PSP/PFSP and useful for setting up the strategies of a national maritime security policy ........................................................ 74
3.2 Objectives of the individual papers ...................................................................... 74

4. Materials and methods ......................................................................................... 77
4.2 Paper 2: Opening of offshore oil business in Mexico and associated framework to cope with potential security risks ............................................. 81
4.3 Paper 3: Enhancing maritime security in Mexico: Privatization, militarization, or a combination of both? ..................................................... 81
4.4 Paper 4: Mexico's reorganisation of maritime security regime: A new role for the navy and emphasis on energy related infrastructures .............. 82
4.5 Paper 5: Integrating the procedures of reporting port security incidents and the follow-up investigation to build a national maritime security policy: A case study in Mexico ...................................................... 83
4.6 Scope & delimitations ........................................................................................... 84
4.7 Validity and reliability .......................................................................................... 85

5. Results ...................................................................................................................... 89
5.1 Paper 1: Implementation and compliance of the International Ship and Port Facility Security Code in Mexico: A literature review and selected issues ............................................................................................................. 89
5.2 Paper 2: Opening of offshore oil business in Mexico and associated framework to cope with potential security threats ..................................................... 90
5.3 Paper 3: Enhancing maritime security in Mexico: Privatization, militarization, or a combination of both? .................................................................90
5.4 Paper 4: Mexico's reorganisation of maritime security regime: A new Role for the navy and emphasis on energy related infrastructures ...91
5.5 Paper 5: Integrating the procedures of reporting port security incidents and the follow-up investigation to build a national maritime security policy: A case study in Mexico .................................................................93

6. Discussion and conclusions ..............................................................................101
  6.1 Evaluating the need of expansion to apply the ISPS Code to passenger ferries of less than 500 GRT and its respective port facilities ..................101
  6.2 The inherent role of the ISPS Code in keeping ports and vessels free of illegal traffic of drugs, weapons and unlawful items & the use of the developed transparent tool for reporting of security incidents and development of a national maritime security policy .....................................103
  6.3 The need for expansion of the ISPS Code to offshore facilities in Mexico ........................................................................................................107
  6.4 The enactment of the ISPS Code into Mexico’s national legislation, the 2016 maritime reform and possible solutions to juridical ambiguities 109
  6.5 Conclusions and recommendations ..........................................................112
  6.7 Further research ..........................................................................................114

References ............................................................................................................ 117

Appendix .............................................................................................................. 123
Acknowledgement

To study maritime security and particularly port security, including areas as terrorism, robbery at sea and illegal transportation of weapons, drugs, and explosives, as a relatively young woman, has not been an easy journey. The gender prejudices came to surface whenever I was asked about my area of research.

Questions like, -“Really, do you study maritime security?” were normal at international conferences. However, the unlimited support of my supervisor, Dr. Dimitrios Dalaklis and his unrestricted sharing of expertise, helped me to navigate away from gender discussions and guide them to my interest areas: Maritime Safety and Security. Thus, I want to thank him from the bottom of my heart. Professor Dimitrios, thank you for accepting to take me as your PhD student, for guiding and advising me throughout this journey. For calming me down when I panicked and for getting me back on track to fulfil the research. Thank you for keeping me in focus, when I was furious because of discussions about gender issues and its limitations in maritime security. Thank you for understanding me when things got hard, guiding me out of stormy waters and back on route. Thank you for your constructive criticism, helping me improve the articles and thank you for co-authoring the papers appended to this dissertation.

The research topic demanded access to the military/naval world, the customs world, the merchant marine and ports world to examine the level of implementation and compliance of the International Ship and Port Facility Security Code in Mexico. This, alone, appeared to be a mammoth task. But it was not; thanks to Rear Admiral Germán Álvarez Lobato, who helped me gain access to the source. I can never thank him enough for helping me and guiding me with the process of gaining access to the Mexican Navy. The research could never had been carried out if the Admiral Vidal Francisco Soberón Sanz, Secretary of the Secretariat of the Navy in México, had not granted access. Therefore, I would like to express my deepest gratitude to him, as well as to Admiral Ángel Enrique Sarmiento Beltrán, Under-Secretary, who patiently helped and supported me with my research stay in Mexico and facilitated the implementation of the “transparent port security incident reporting tool” and analysis of its results. I know very well that it is not easy to allow an outsider into your world and let her interview the selected persons without censure. Thank you both for allowing this research, which goals resemble yours: improving port and maritime security.

I would further like to acknowledge all the interviewed persons at the different ports in Mexico while conducting the study: Harbour Masters, Admirals Commanders of the Mexican Navy, Commanders of the Mexican Navy Units with duties of Coast Guard (UNAPROPS), Directors of Customs Maritime Units, Port Facility Security Officers and Port Directors. Thank you all, for openly answering the questions in
my long interviews. Due to ethical rules, I am not allowed to provide here your names. Anyhow, I want to express my sincerest gratitude to all of you for your kindness and for letting me perform participant observation at your working places. Thank you for allowing me into the Customs areas, for making the necessary arrangements so I could be an observer on board navy patrols. Thank you for letting me visit the different areas of all the ports visited the Harbour Masters installations and port and vessel traffic centres. Thank you all for the fruitful discussions that helped me to shape my work.

Sincerest thanks must also be provided to all members of the WMU PhD progression board. Thank you all for helping me along the way. Special thanks goes to professors, Aykut I. Ölcer, Michael Baldauf, Raphael Baumler, Momoko Kitada, Michael Ekow Manuel, George Theocharidis, Neil Bellefontaine, María Carolina Romero Lares, Henning Jessen and Larry Hildebrand for attending all my PhD progression seminars, keeping track of the research and enriching my work with their comments among their areas of expertise.

My heartfelt gratitude goes to Professor Max Mejia, Director of the PhD Programme and Head of Maritime Law & Policy, who lead the progression seminars for focusing the discussions into the research topic allowing me to shape and improve the study. Thank you also for sharing invaluable expertise on the subject and lending me relevant bibliography to enrich my study. Thank you for being a source of not only knowledge and expertise, but also inspiration.

Thanks to the WMU Library staff – Mr Christopher Hoebeke and Anna Volkova for assistance in sourcing information and invaluable guidance in selecting relevant bibliography. Thanks to Carla Fisher for kindly helping me with all administration during my PhD and for continued support. Thanks to Stephen Humlen-Grinstead for correcting my English in this dissertation. Thanks to the remaining WMU staff and students for giving me the pleasure of interacting with you during this journey. Thank you to the CONACYT, in Mexico, for funding the research.

Thank you to the President of WMU, Cleopatra Doumbia-Henry, for being of motivation, lightening the path bringing amazing personalities to conferences at WMU, from which I enriched my work.

My deepest gratitude to Øystein Nordfjeld for supporting me through this journey being an amazing father while I was away. Thank you for taking care of our most precious treasure and beloved son. Sebastian, I dedicate this doctoral dissertation to you, my biggest source of motivation and the only one that always manage to colour life when it turns blue.

Finally, to my wonderful home country, Mexico. I hope to contribute into improving security in the Mexican territorial waters and Mexican ports with this dissertation. Worldwide impact is also aspired.
Abstract

The issue of port security raised concerns at the highest levels after the terrorist attacks on September 11, 2001 against the United States. Security threats against ports and vessels acquired a new perspective and in 2002 the International Maritime Organization (IMO) adopted amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, introducing Chapter XI-2 - Special measures to enhance maritime security. This set of regulations enshrines the International Ship and Port Facilities Security Code (ISPS Code), which entered into force on 1 July 2004.

This Code establishes a set of measures to enhance the security of ships and port facilities. It encompasses two parts. Part A establishes the mandatory provisions, the non-mandatory (“recommended”) and part B provides guidelines about how to comply with the obligatory requirements of part A. Together with a critical analysis of the national legislation about the enactment of the ISPS Code into national law, this dissertation examines the level of implementation and compliance of this instrument in Mexico with special focus on port security. This dissertation also provides a transparent incident-reporting instrument developed and tested through this research effort in Mexico for reporting of port and maritime security incidents.

This tool joins three primary port/maritime security functions:

a) Reporting of port and maritime security incidents;

b) Classification and investigation of serious security incidents that require reassessments of the Port Security Assessments, (PSA), Port Facility Security Assessments (PFSA), and amendments to Port Security Plans (PSP) and Port Facility Security Plans (PFSP) and finally;

c) Collection of evidence material related to the security incident.

This instrument, combined with statistics, provides nations with crucial information, about threats, needs and challenges for allocation of economic, material and human resources. It also provides essential information material to set up strategies for the development of a National Maritime Security Policy. Its flexibility and adaptability makes possible its implementation at any State of the world.

The results of this analysis reflect the conflictive cooperation between the Secretaría de Marina (SEMAR)\(^1\), and the Secretaría de Comunicaciones y Transportes, (SCT)\(^2\). This, together with the ambiguities and contradictions of the National Maritime Regime, even though the extensive reforms of 2016 limits the exercise of authority

---

\(^1\) Secretariat of the Navy, in English.

\(^2\) Secretariat of Communications and Transportation, in English.
of SEMAR and the operation of the CUMAR(s), the organ responsible for implementation and compliance of the ISPS Code, at all ports across the country. This doctoral dissertation comprises six introductory chapters, which are referred to as the kappa and five annexed papers. It aims to contribute to the maritime realm within the area of maritime security, with special focus on port security through the following general objectives:

- Elaborate a critical analysis of the current port security situation of Mexico, with special focus on implementation and compliance of the ISPS Code, including the state of the art and harmonization of international legislation with national law;

- Identify the most relevant security threats to port facilities in Mexico, including oil terminals and offshore installations;

- Develop an analytical instrument for security incidents-reporting & incident investigation, to strengthen the continual evolution of PSA/PFSA and PSP/PFSP and useful for setting up the strategies of a national maritime security policy with possibility for implementation worldwide.

The approach adopted in this study is mainly based on qualitative methods, combined with action research and a limited use of statistics. The research objectives call for classical documental analyses examining the elements of relevant international legislation against its implementation into national legislation in the referred nation-state. The methods were selected on their usefulness and efficacy for analysis of law and policy. Action Research was used for implementation test and improvement of the reporting incident instrument, which can also be used for setting up the strategies for the development of a National Maritime Security Policy. Action Research is recommended when it is intended to improve understanding, develop his/others learning and influence other’s learning, taking action for social improvement.

The findings related to serious deficiencies in the implementation and compliance of the ISPS Code in Mexico, concerning reporting of security incidents and its re-evaluation with the PFSA and respective amendments to PFSP, the poor exercise of authority from the representatives of SEMAR at the CUMARs in respect of fulfilling its obligations and responsibilities concerning port and maritime security; and the identification of necessary legal amendments to national law, as well as the remarkable improvement in reporting security incidents after the implementation of the “transparent security-incident-reporting tool”, that enables port/maritime security incident investigation and can serve to identify the problem areas; contributing to set up the strategies for the development of a national maritime security policy, together with the instrument itself, are some of the most relevant contributions of this dissertation.
Abbreviations

- AIS: Automatic identification System
- CCTV: Closed-Circuit Television
- CSO: Company Security Officer
- CSR: Continuous Synopsis Records
- CUMAR: Centro Unificado para la Protección Marítima y Portuaria (Unified Centre for Port and Maritime Security, Mexico, own translation)
- DOF: Diario Oficial de la Federación, in Spanish (Official Diary of the Federation, in English)
- DoS: Declaration of Security
- EEZ: Exclusive Economic Zone
- FIDENA: Fideicomiso de Formación y Capacitación para el Personal de la Marina Mercante Nacional, in Spanish (Fund of Education and Training for the National Merchant Marine, in English, own translation)
- IMO: International Maritime Organization
- INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (National Institute of Transparency, Access to the Information and Protection of Personal Data)
- ISM: International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code)
- ISPS Code: International Ship and Port Facility Security Code
- ISSC: International Ship Security Certificate
- MODU: Mobile Offshore Drilling Unit
- MoU: Memorandum of Understanding
- PFSA: Port Facility Security Assessment
- PFSo: Port Facility Security Officer
- PFSP: Port Facility Security Plan
- PSA: Port Security Assessment
- PSAC: Port Security Advisory Committee
- PSC: Port Security Committee
- PSO: Port Security Officer
- PSP: Port Security Plan
- RSO: Recognized Security Organization
SCT – Secretaría de Comunicaciones y Transportes, in Spanish, Mexico (Secretariat of Communications and Transportation)

SEMAR – Secretaría de Marina, in Spanish, Mexico (Secretariat of the Navy)

SOC – Statement of Compliance

SOLAS – International Convention for the Safety of Life at Sea, 1974

SSA – Ship Security Assessment

SSAS – Ship Security Alert System

SSO – Ship Security Officer

SSP – Ship Security Plan

STCW – International Convention on Standards of Training, Certification and Watch keeping for Seafarers, 1978


UN – United Nations

UNAPROP – Unidad Naval de Protección Portuaria, and represented with the abbreviation UNAPROP, in Spanish, in Mexico (Navy Unit for Port Protection, own translation)


WCO – World Customs Organization
List of figures

Illustration 1 Security incidents at oil platforms January-September 2016, area of Tabasco by month.............................................................................................................. 63
Illustration 2 Security incidents at oil platforms, January-September 2016, area of Tabasco by oil facility ...................................................................................... 63
Illustration 3 Security incidents at oil platforms January-September 2016, area of Tabasco, by type of incident................................................................. 64
Illustration 4 Cuts to monitors and fire prevention equipment.......................... 65
Illustration 5 Model for port and maritime security incident investigation........ 77
Illustration 6 Action-reflection cycle (Mcniff, 2011).......................................... 79
Illustration 7 Graphic of port security incidents by quarter.............................. 96
Illustration 8 Graphic of port security incidents by incident code.................... 97
Illustration 9 Port security incidents by quarter and port area.......................... 98
Illustration 10 A very small ferry sailing in a restricted waterway in a maritime oil port facility, in Mexico ................................................................. 102

List of Tables

Table 1 Number of litres of crude oil stolen, 2014 ........................................... 58
Table 2 Number of litres of crude oil stolen 2015 .......................................... 58
Table 3 Pemex employees prosecuted for theft of hydrocarbons, 2014-2015..... 59
Table 4 Number of illegal connections to Pemex's pipelines discovered, 2014-2015 ........................................................................................................................... 59
Table 5 Number of employees/ex-employees investigated for theft of hydrocarbons per year. Period 2006-2015. Source Pemex answer to INAI, SISI 1857200171515 .................................................................................................................. 59
Table 6 Number of employees arrested theft of hydrocarbons by working division. Source Pemex’s answer to INAI, SISI 1857200171515......................... 60
Table 7 Pemex's employees investigated for other crimes, 2006-2015............. 61
List of papers included in this dissertation

The list of papers and respective presentation of articles does not follow a chronological order after the publication date (those with empirical data were approved and published earlier than those focused on theoretical analysis). Instead, the discussion of the papers is conducted under the approach of the background information in relation to the development of the research topic. This, to provide a comprehensible sequence of analysis of theory and data. Following this approach the literature review is presented in paper 1. The justification of the problem is presented in Paper 2, whereas the analysis of empirical data and recommendations are presented in paper 3, 4 and 5, from different perspectives.


This paper provides a literature review of the state of the art on implementation and compliance of the International Ship and Port Facility Security Code (ISPS Code), for the case of Mexico. This investigation was initially oriented solely towards Mexico, but due to the absence of research within this subject for the referred country the review had to be done through subcategories with the conditional connection of Mexico and relevant issues were selected. The primary data confirmed the absence of research within this subject in Mexico. The secondary data, is related to the ISPS Code used for the search, and allowed for a wider geographical coverage and expanded on general basis the scope of the analysis. Ten (10) different academic databases were exploited. The literature review from an author centric approach is initially presented; then, it is used as the basis to further develop (and examine) the concept centric approach through eight selected categories. The careful screening of literature, constructed on specific concepts allowed the identification of cross fertilisation of such concepts in the respective fields. It is observed that the research efforts focused on the ISPS Code and the development of a Port Facility Security Plan (PFSP) have an integrated perspective where the categories of terrorism and counterterrorism, as well as maritime security management and the issue of port security have a strong interaction and dominant status. The results demonstrate the limited number of academic contributions in the areas Central and South America and in relation to other parts of the globe, as well as the total absence of research efforts about the ISPS Code in Mexico. In the scientific contributions on the subject where Mexico is included; it is in reference to isolated cases of armed robbery, drugs
organizations or proliferation of crime on general bases, but not regarding the ISPS Code itself. The absence of scientific research on this area for the specific country might also be related to the lack of a national maritime security policy and a poor maritime security culture as the authors have pointed out in other contributions.


After 75 years of State oil monopoly, Mexico performed the first business oil auction in 2015 involving the private sector. This auction offered 14 oil exploration fields located on the Continental Shelf to private companies. The development and exploitation of these hydrocarbon fields face significant challenges regarding security. The economic loss for theft of hydrocarbons through illegal connections to pipelines is estimated to 973 million, 125 thousand U.S. dollar, for the year of 2014 alone. While productive research has been made, it has mainly focused on transportation systems and basically, pipelines. The development and establishment of policies prioritising maritime security and protection of critical offshore infrastructure against theft of hydrocarbons, drugs organizations and terror attacks needs to be included in the national agenda to improve maritime security and mitigate potential security risks at sea. This could increase the trust of investors and stakeholders and would contribute to the faster development of new exploration and production fields. While the International Ship and Port Facility Security Code (ISPS Code) is the cornerstone for the construction of the port’s security program and establishes the requirements of the Port Facility Security Plan (PFSP), including oil port facilities, has not been fully implemented in several important Mexican ports. It is concluded that some important ports lack many of the core security processes, procedures and controls that should be included in any PFSP. This article briefly reviews the situation of the oil industry from a security perspective and discusses key elements of maritime security; addressing the necessity of the inclusion of maritime security and the protection of critical oil infrastructure offshore in the national agenda which would provide for future research directions in the maritime security domain and contribute to the establishment of a national maritime security policy.
The current analysis examines three different options/solutions that Mexico implemented within its ports and offshore installations in order to improve the country’s maritime security framework, as well as ensuring compliance with the International Ship and Port Facility Security Code (ISPS Code): privatization, militarization and finally, their combination. Findings of an ongoing research effort include inconsistencies within the data of the necessary security incident records, or even their total absence; inadequate competence and training among the Port Facility Security Officers (PFSO) also stands out. Another important issue was the use of different procedures among the ports under investigation for dealing with exactly the same security issues. The clear conclusion is that after twelve years of the ISPS Code implementation, Mexico, which is leading the Inter American Port’s Commission of the Organization of American States (OAS), does not comply with the requirements of the ISPS Code at an acceptable level; the lack of a national maritime security policy has resulted in a poor (maritime) security culture, despite the severe (security) challenges that this nation is facing. It is also true that the country under discussion is currently reorganizing its maritime security apparatus with some positive results; tools/recommendations for enhancing the Mexican maritime security operating framework are therefore provided, along with areas of potential future research.

International Maritime Organization’s (IMO) member-States have a strong and invested interest in securing their energy supply routes and interrelated ports. Preventing incidents in relation to this type of infrastructure is essential for commerce and requires careful planning and rigid actions. Apart from ensuring the optimal use of energy resources through energy efficiency initiatives and policies, eliminating (or, at least reduce) losses that are related to theft and/or subversive actions associated with terrorism is essential for national security reasons. The legal framework used by the United Mexican States government to shift the National Maritime Authority
from a civil institution (Secretariat of Communications and Transportation, in English and referred to as SCT hereafter) towards a military one SEMAR (Secretariat of the Navy, in English and referred to as SEMAR hereafter) provides the starting point of the analysis at hand. Previous failures of the country’s Maritime Designated Authority are associated with an extended number of security incidents and various accidents. In an attempt to improve the country’s maritime safety and security regimes, a relevant Presidential Decree approved in December 2016 transferred the oversight of all Harbour Masters from SCT to SEMAR. Research activities on the field testify that this initiative achieved high acceptance rates between the four pillars of representatives of authorities/institutions directly related to duties and operations within these two important domains, a prerequisite for success. Apart from the recent Decree, extensive reforms to several laws are still necessary to ensure an improved maritime security apparatus. The National Congress heavily focused on port security and rather neglected to consider that part of the International Ship and Port Facility Security Code (ISPS Code) regarding Ship Security Plans and all its related subjects to vessels since the previous reform, in 2014. It is also noteworthy that the Decree is unnecessarily complicating the tasks of the Maritime Authority; while it designates the SEMAR as the National Maritime Authority, it provides the tasks of Port Authority (including port state’s privileges and obligations) to SCT. This could potentially impact negatively on the conduct of operations in the future and indicates a need of improvement in the implementation process of IMO’s instruments into national legislation. Amendments to regulations concerning security of Mobile Offshore Drilling Units (MODUs) and other offshore installations should also be considered to be included in the type of vessels obliged to comply with the ISPS Code, since a poor security situation in the specific category also strongly affects the Mexican oil energy market.

5) Ávila-Zúñiga-Nordfjeld, A. & Dalakis, D., 2018. Integrating the procedures of reporting port security incidents and the follow-up investigation to build a national maritime security policy: A case study in Mexico. Accepted for publication by the WMU Journal of Maritime Affairs (in press, 2018).

Developments within both the maritime and port security domains are regulated by international standards, with the influence of the International Maritime Organization’s (IMO) International Ship and Port Facility Security Code (ISPS Code) clearly standing out. The analysis at hand is putting forward the idea to improve port security measures in developing
countries via integrating the procedures of incident reporting and the associated follow up investigation, hinging on the Mexican experience. The specific research effort examined port security at Mexican ports; Harbour Masters, Commanders of the Mexican Navy as representatives from the CUMAR, Directors of Customs Maritime Units, Port Facility Security Officers and Port Directors were interviewed on the subject in order to identify the challenges and opportunities for security incident reporting, updating of security incident records and facilitation of the follow up investigation. Then, a qualitative security model was developed; under this new framework, incident reporting, incident investigation, the reassessment of security threats through the Port Facility Security Assessment (PFSA) and the necessary modifications to the Port Facility Security Plans (PFSP) were all integrated. These subjects were all incorporated into a “transparent port security incident reporting tool”. This tool was then implemented at all ports in Mexico where the ISPS Code applies, by the National Maritime Authority. This demonstrated in a real case through “action research”, the improvement of port security framework in the country. Measurements were executed every quarter throughout the year 2017 and the incident-reporting instrument was adjusted accordingly. The results demonstrated a significant improvement in reporting security incidents, with the increase from absolutely nothing (zero) to 57 providing a strong indicator of success. In addition, 56% of those reported maritime incidents were also associated with recommendations to be integrated into the PFSA and respective PFSP. Collecting accurate and immediate information/evidence material while reporting security incidents is crucial for effective incident investigation and continuous improvement of the PFSP.
Other works by the respondent


The analysis in hand conducts an assessment of the need of implementing the International Ship and Port Facility Security Code (ISPS Code) instruments, from the International Maritime Organization (IMO) and particularly the Port Facility Security Assessment (PFSA) and Port Facility Security Plan (PFSP) at Customs Maritime Units. This research effort examines the security at Mexican Customs Maritime Units’ installations at different ports from the ISPS Code perspective. To study these phenomena, Harbour Masters, the Commanders of the Navy, Directors of Customs Maritime Units, Port Facility Security Officers and Port Directors from eighth of the most important Mexican maritime ports were interviewed on the subject to identify the challenges and opportunities for improving maritime and port security. Additionally, the Customs Maritime Units’ installations were visited for direct observation. The results demonstrate the negative effect of customs agents rotation between Customs Airport Units, Customs Border Units and Customs Maritime Units, as well as the need for the development and implementation of PFSAs and PFSPs not only at ports and port terminals, as required by the ISPS Code; but also at the Customs Maritime Unit’s installations, which are within the port installations. The findings show that more than 40% of port and maritime security incidents occurred at the Customs installations during the year of 2017, in Mexico. The lack of security assessments and security plans at Customs Maritime Units put at risk the whole port facility and its terminals. Therefore it is recommended the establishment of a national department within the Customs Authority to lead the development of security assessments and security plans but in accordance with the specifications of the ISPS Code, aiming for a harmonization between “Customs Security Plans” and PFSP, in order to establish security procedures at Customs Maritime Units that are synchronized with those from the port facility in case of serious security incidents. Finally, it was identified the urgent need for providing maritime and port security training related to ISPS Code requirements and procedures to customs’ police personnel serving in Customs Maritime Units.
Theoretical and practical implications are discussed for researchers and practitioners in the areas of maritime security and future research directions are provided.
1. Introduction

“They [PFSP] may exist in paper form but are rarely pulled off the shelf to test their effectiveness. The key to successful port security management in terms of the FSP is to understand it as a living document. (...). The FSP should not be written as a one-time effort, but should truly be a working document that addresses the security threats facing the port facility twenty-four hours a day, seven days at week. This means that the FSP, like the security function itself, must be continually updated and tested to be certain that it mitigates the threats identified in risk assessment”.

-Kenneth Christopher (2009).

Concerns about maritime security have grown heavily during last decade due to the increase in terror attacks around the globe, as pointed out by Christopher K. (2009), who said that “the evolution of organized security processes in the maritime sector can be understood as a product of increasing governmental and commercial concerns about the criminal exploitation of seaports, [...] and the rising threat of global terrorism”. Maritime and port security is a topic that has been discussed for several decades at the International Maritime Organization (IMO) and that received exceptional attention after the terrorist attacks on September 11, 2001, against the United States of America, who immediately adopted the highest security measures to protect its ports and infrastructure.

In 2004, after the referred tragic events of September 11th, 2001, the IMO established a set of maritime security regulations with the aim of improving maritime and port security worldwide. These provisions are established in the new Chapter XI-2 of the Safety of Life at Sea Convention 1974, (SOLAS Convention), comprising the International Ship and Port Facility Security Code (ISPS Code). Part A of the ISPS Code establishes the mandatory provisions, while the non-mandatory (“recommended”) part B covers guidelines about how to comply with the mandatory requirements established in part A. However, implementation and compliance of the ISPS Code and submission of related information is only mandatory for Contracting

---

3 IMO – the International Maritime Organization – “is the United Nations specialized agency with responsibility for the safety and security of shipping and the prevention of marine pollution by ships” (IMO official website, 2018).
Governments to the SOLAS 1974 Convention\(^4\). The IMO relies on market forces and economic factors to ensure compliance of the ISPS Code and therefore, there is no penalty mechanism for Contracting Government States that do not comply with the ISPS Code requirements (official website IMO, SOLAS 1974). After almost 14 years of the ISPS Code implementation, market forces and economic factors have not been sufficiently powerful to lead to full compliance in several countries around the world. One of these is Mexico, where, at the time when this research effort was conducted, serious deficiencies were detected.

The focus of recent research regarding maritime security has been on piracy at sea, while port security and security of offshore installations has not received the same attention, even when offshore installations have been defined by several researchers as vulnerable strategic infrastructure [Lewis (2006); Espin-Digon, Burns-Herbert, & Bateman (2008); Weinberg (2008); Christopher (2009); Schulz (2011)]. Yet, maritime and port security has not been considered seriously enough in the national agenda in Mexico, a country that have suffered several tragic incidents caused by organized crime stealing oil and gas from oil installations, including oil terminals at ports where drugs, weapons, psychotropic material and money in containers, have illegally been transported in ships and continuously confiscated. In this nation, the topic remains widely unexplored from the academic perspective as well, as discussed in Paper 1 and Paper 2 of this dissertation.

Even if Mexico does not comply with the ISPS Code at a satisfactory level, a significant improvement is recently recorded. During the course of this research effort a lot of improvements to harmonize the maritime legislation with maritime politics have already been carried out, including the legislative initiative presented by the President of Mexico and approved by the National Congress to reform the country’s maritime legal framework and allow the shift of maritime safety and security responsibility, as well as Port State Control from a civil authority (SCT)\(^5\) towards a military one (SEMAR)\(^6\), which entered into force on 17th June, 2017. This maritime reform was recommended by the researcher in Paper 3 prior for its approval. The reform transferred the control of all Harbour Masters, from SCT to SEMAR, which set the SEMAR under structural organizational changes to cope with its new responsibilities and duties. However, as discussed in Paper 4 of this dissertation, the international legislation concerning the ISPS Code is not fully enacted or adopted into national law, which limits the strategies of SEMAR to cope with maritime security threats. Despite the extensive maritime reform that enter into

\(^4\) The SOLAS Convention is usually referred to as “SOLAS, 1974, as amended”. It is addressed as the most important of all international conventions concerning the safety of merchant ships.

\(^5\) The Secretariat of Communications and Transportation, in English, and referred to as SCT here thereafter.

\(^6\) The Secretariat of the Navy, Secretaría de Marina (SEMAR) in Spanish, and referred to as SEMAR here thereafter.
force in 2017, there is still an urgent need of new reforms to national legislation in México, to include the part of the ISPS Code related to security of vessels, like appointing of Ship Security Officers (SSO), development and approval of Ship Security Assessments (SSA) and implementation and compliance of Ship Security Plans (SSP), as explained in paper 4 of this dissertation. This research contribution not only set light on the need of adequate security training of Port Security Officers (PSO), Port Facility Security Officers (PFSO) and port security authority representatives from the CUMAR\(^7\), but also in the poor knowledge about the maritime domain on the part of legislation drafters and the National Congress representatives.

The poor performance of the previous Designated Authority (SCT) to comply with its obligations under international Conventions from the IMO was documented by the researcher in Paper 3, 4 and 5 from various perspectives. SEMAR has been responsible for maritime security, including implementation and compliance of the ISPS Code since the previous maritime reform of 21st April, 2014, when the presidency of the CUMAR was transferred from Harbour Masters to the Admirals, Commanders of the Navy sector, zone or region for the specific port. Their duties included inspection, revision and approval of Port Security Assessments (PSA), Port Facility Security Assessments (PFSA), Port Security Plans (PSP), and Port Facility Security Plans (PFSP) at the appropriate maritime security levels. Due to absence of cooperation between SCT and SEMAR, Harbour Masters did not explain or comment on the changes to Admirals and representatives from the CUMAR, who’s lack of knowledge and poor training, resulted in becoming unaware of their duties and responsibilities due to these changes. Maritime and port security were left in a vulnerable situation for a period of almost three years from 2014 to 2017, when the last reform entered into force. These findings as well as poor development of PSA, PFSA and PSP, PFSP are among the findings presented in Paper 5 of this doctoral dissertation, which were discovered as a result of several research visits to different ports in Mexico, where the five pillars of port and maritime security were interviewed, including Harbour Masters; Commanders of the Mexican Navy and functioning as Presidents of the CUMAR; Directors of Customs Maritime Units; Commanders of the UNAPROP (Navy Unit for Port Protection with duties of Coast Guard, Unidad Naval de Protección Portuaria, in Spanish, represented with the acronym UNAPROP, and called with this acronym here thereafter); Port Administration Directors, Port Security Officers (PSO) and Port Facility Security Officers (PFSO).

\(^7\) Centro Unificado para la Protección Marítima y Portuaria and represented with the acronym “CUMAR”, in Mexico, in Spanish and will be referred to as CUMAR here thereafter. It could be translated to “Unified Centre for Port and Maritime Security”, but there is no official translation.
These serious findings thoroughly discussed in Paper 5, are central to the topic of this doctoral dissertation. Another aspect is that due to the gravity of those findings, the researcher decided to make a further effort to integrate action research to the study in a determination to contribute improving port and maritime security in Mexico.

In 2017 important solutions were implemented. ISPS Code related training was provided to Commanders of the Navy, functioning as Presidents of the CUMAR and Commanders of the UNAPROP, who were made aware of their duties and responsibilities related to the ISPS Code first by the researcher and later directly by the International Maritime Organization, upon requirement of the National Maritime Authority, in México, SEMAR.

The National Maritime Authority implemented at all ports the transparent incident-reporting tool, developed by the researcher. This brought a significant improvement on increasing reporting of incident security incidents and updating of incident security records, increasing from zero to 57, during the first year of its implementation; the redacted PSP and PFSP were requested and are under revision by representatives of the CUMAR.

These actions implemented by the Maritime National Authority were to a certain extent harmonized with the aim of this dissertation, which was first to contribute to the maritime world by developing a tool that could be used to set up the strategies at a macro level for building a national maritime security policy in any Contracting State to the SOLAS Convention around the globe, and at the same time, improve security incident reporting and incident investigation. Secondly, to implement it in Mexico, testing its usability, improving it through systematic periodical measurements to assist the referred country in this duty and offer it to the world. This was achieved through several phases of research work, which included examination of the national legal framework for port and maritime security related to the enactment of the ISPS Code into national legislation; second, to analyse current security threats at Mexican ports and oil terminals at port facilities and finally; to contribute to the understanding of the value of reporting security incidents and updating of security incident logs through the use of “action research” and the implementation of the referred tool above.

Emphasis was also put in the value of reporting incidents classified as “serious,” as well as results of security drills and exercises for reassessment of PSA/PFSA, with the consequent amendments to PSP/PFSP, recalling that such changes must be tested and updated accordingly to manage security threats and maintain the security of the port at an acceptable level.

As mentioned in the abstract, this doctoral dissertation encompasses six (6) introductory chapters referred to as the “kappa”, in addition to five (5) annexed
papers, which are the result of research conducted over the last three years. Chapter one contains this overall introduction to the research presented in this document. It is followed by relevant background information presented in Chapter 2. Objectives are presented in Chapter 3 while research methods and instruments used in this research are explained in Chapter 4, followed by Chapter 5 presenting results and findings. General discussion and conclusions are discussed in Chapter 6, including future research directions.

Two of the annexed papers to this kappa have been published as book chapters, one more was published in an international peer review journal, and two more were published in an international journal. Another one has been submitted to another international peer review journal and is currently under review.
2. Frames of reference

The following subsections cover relevant background information to understand the importance of this research and its contributions and provide the adequate context to the objectives of this dissertation, which will be presented in Chapter 3. The subsequent subsections present international legislation related to port and maritime security, national legislation in Mexico related to the same topic, current threats to port and maritime security for the case of Mexico and finally, the value of testing and updating PFSP through sufficient security drills exercises and after assessment of serious incidents.

2.1 International legislation for port and maritime security

Maritime security has been defined as “the state of being free from the threat of unlawful acts such as piracy, armed robbery, terrorism, or any other form of violence against ships, crews, passengers, port facilities, offshore installations, and other targets at sea or in coastal areas” by Mejia, (2007). As it is observed, port security is incorporated to the different areas of maritime security. Under this approach, port security can be understood as the state where a port facility, including its terminals, personnel and all its related infrastructure, as terminal berths and navigations channels, vessels at the port, its crew, passengers, service providers during operations at the port, Customs Maritime Units and in general, customers of the port, are free from any unlawful act of violence such as terrorism, sabotage, armed robbery and illegal transportation of drugs and weapons among others.

A difference between “port security” and “maritime security” as two different study areas is appointed for the purpose of this dissertation. However, even if both concepts involve different type of risks or threats, in practice they are interdependent. This research effort will mainly focus on the part of port security.

Among the lessons from the terror attack of September 11th, 2001 is that terrorist are acquiring a higher level of training and coordination required for aviation and maritime targets. Even if land-based infrastructure represents a higher security risk and probability factor than terror attacks to the port industry as bomb threats or other
scenarios like sinking a vessel in navigation channels, or using it as a weapon against the port facility or oil terminals, among others, these are not impossible. Neither is the fact of using the ship to smuggle drugs or weapons.

Jones (2012) argues that “port facilities are inherently vulnerable because they must provide access by land and sea and because they are sprawling installations, often close to population centres”. The referred author adds that smuggling of drugs, contraband, weapons or other illegal products and goods is a well-established security threat to shipping and highlights the inherent duty of the master to keep the vessel free of illegal items, pointing out the importance of the relationship between the charterer and the Port Facility Security Officer in safeguarding both the vessel and the port facility. Where there is a suspicion of smuggled unlawful items onboard the vessel, a search regime must be carried out.

To keep the port facility, including its berths and navigation channels on one side and vessels on the other side, free of drugs and weapons is a shared responsibility from the ship’s Master and the PFSO. The ISPS Code has addressed the risks of smuggling items at the interface between the vessel and the port facility and establishes the responsibilities and duties of each of the parts for these port operations. However, cooperation between both sides is a prerequisite to achieve to manage properly such situations.

Huge differences in security levels can be found at different ports even within the same country. These differences in security are even more evident when studying ports in different geographical areas. Non the less, some elements of physical security must be included in general at all ports to comply with minimum international standards concerning security measures established by the ISPS Code, regardless of its location. The elements that must be considered in the development of PSA/PFSA and PSP/PFSP include an effective port perimeter security, surveillance and patrols, as well as strict access controls by sea and land, Intruder Detection System (IDS), CCTV systems to keep control over sensitive areas, metal and explosives detectors and establishment of security procedures.

As Jones (2012) explains, “a port security regime also needs to be able to assess the security implications of cargoes and shipments inside, or arriving at, the port. This involves investing in X-Ray technology and scanners to pick up security breaches such as people, drugs, explosives, radiation and illegal shipments”.

Considering that security risks can be reduced to an acceptable level through implementation of security measures, but never be totally eliminated, the candidate defines port security as the comprehensive set of security measures and instruments implemented at a port, after security risks has been assessed appropriately, continuously and systematically in relation to the port facility (including its terminals, personnel, service providers, customers and all its related infrastructure)
through security risks assessments, security drills, exercises and the fully implementation of a security plan; to manage threats and mitigate results of security incidents.

In reality, there is no port around the world that can claim to be 100 per cent free of security threats and, therefore, it is necessary to have performed a PSA/PFSA and have implemented a PSP or PFSP, for port terminals, with all its related procedures and security measures to respond to security incidents and mitigate the results of unlawful actions that threaten the security of ports, port terminals, personnel, maritime customs facilities, vessels, and the public in general.

2.1.1 The International Ship and Port Facility Security Code (ISPS Code)

Concerning maritime security, one of the most important instruments of international law is the set of maritime security regulations developed by the IMO, after the tragic events of September 11th, 2001. These provisions were established in Chapter XI-2 of the Safety of Life at Sea Convention 1974, (SOLAS Convention), containing the ISPS Code. This Code is defined by the IMO as “the comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States” (International Maritime Organization, 2012). Whereas part A of the Code establishes the mandatory provisions, the non-mandatory (“recommended”) part B comprises guidelines about how to comply with the mandatory requirements of part A.

Paper 3 of this dissertation makes it clear that the ISPS Code “only apply to passenger ships, high speed passenger vessels and cargo vessels of 500 gross tonnage and upwards; as well as Mobile Offshore Drilling Units (MODUs) in transit and at ports (but not to fixed and floating platforms and MODUs on the oil field); and all type of port facilities serving vessels offered for international voyages”. It is also explained in Paper 3, that, “the extent to which the guidelines apply on ships will depend on the type of the ship, its cargo and number of passengers, as well as its sailings routes and the features of the port of or port facilities visited by that specific ship. Regarding the application of guidelines to port facilities, it will depend on the type of carriages and vessels visiting that particular facility and its ordinary trading routes”.

The mandatory Part A of the ISPS Code, describes that contracting governments have to appoint the Designated Authority to carry out certain maritime security duties/responsibilities established in the Code. This Designated Authority holds the responsibility of setting Maritime Security Levels and ensuring compliance with the maritime security measures at all ports (where the ISPS Code apply) through the
PSA and PFSA; the revision, approval and control of compliance of the PSP and PFSP, which shall be based upon the PSA and the PFSA. The development of PSP/PFSP is also within the responsibilities of the PSO/PFSO. The PSO/PFSO must identify critical assets within the port when developing the PSA, and plan for adequate security measures to meet specific needs in case of security incidents.

As established by IMO, there are three different security levels: Security Level 1 (normal) requires the minimum protective security measures at all times. Security Level 2, which requires additional protective security measures for the specific period of time that the risk of a security incident is heightened and Security Level 3, which requires specific protective security measures which shall last only for a limited period of time when risk for a security incident is probable or imminent, even when it is not possible to identify the target. Security Level 3 involves the strictest security measures and its priority is the security of the port, port facilities, vessels and society that may be affected by a security incident and may result in the suspension of commercial operations. Security response under Level 3 is transferred to the government or other organizations responsible for dealing with significant incidents (International Maritime Organization, 2012).

K. Christopher (2009) describes the PFSP as:

“The plan developed to ensure the application of security measures designed to protect the port facility and its serving vessels or those vessels interfacing with the facility, their cargoes, and persons on board at the respective MARSEC levels”.

Christopher correctly points out that the PFSP is the cornerstone for the construction of the port’s security program and includes personnel and physical security systems and processes, access control, security force management and vessel and cargo operations. He emphasizes the need to develop contingency and emergency operations plans and to work efficiently with the federal agencies, port authorities and private enterprises in coordinating both routine and emergency response mechanisms. According to the IMO Guide to Maritime Security and the ISPS Code (2012), threat Level 1 is considered to be “background”, threat level 2 is considered to be “moderate” and threat level 3 is considered as “high”.

However, governments can authorize a Recognized Security Organization (RSO) outside the government to carry out part of their responsibilities regarding the Maritime Security Measures.

Never the less, the level of delegating security duties to RSOs is limited to performance of PSA/PFSA (which must be approved by the government); approval of SSP and subsequent amendments, but only in the case that that specific RSO has not been involved in the development and implementation of the Ship Security Plan; as well as guidance and assistance on security issues, including advices related to SSAs, SSPs, PFSPs and PFSAs. The verification and issuance of the Statement of
Compliance (SOC) for port facilities and International Ship Security Certificates (ISSC) that comply with the requirements of the ISPS Code are responsibilities of the Designated Authority.

Governments are not allowed to delegate the setting of security levels to RSOs. The setting of security levels according to the ISPS Code focuses on the alert for the perceived risk of terrorism attacks, but governments may include other type of threats in their risk evaluation like armed robbery against vessels and platforms. Security levels apply both to ships sailing over their territorial sea and port facilities. The governments can decide on the implementation of different security levels for different ports, port facilities and different areas of their territorial waters. However, the change of security levels must be clearly communicated to port, port facilities and vessels attempting to call that port or port facilities and vessels in transit or attempting to transit those areas.

Other duties which governments are not allowed to delegate to RSOs include the establishment of requirements for the Declaration of Security (DoS); determining the type of port facilities that must appoint a PFSO as well as those facilities that must develop and implement the PSP/PFSP; authorization of PSA/PFSA and amendments, approval of PSP/PFSP and amendments; exercise of control of compliance of security measures of ships with flags from other SOLAS signatory states, and issuance of security certificates to personnel on board ships for compliance of requirements of the International Convention on Standards of Training, Certification and Watch keeping for Seafarers 1978 (STCW) Convention and the STCW Code.

The ISPS Code does not apply to offshore activities. Instead, the IMO has left it up to SOLAS contracting Governments to decide whether to extend its application to Mobile Offshore Drilling Units (MODUs) and to fixed and floating oil platforms, located in the Continental Shelf. Some Governments with high level of offshore activities related to oil and gas exploration and production have developed their own regulations extending the application of the ISPS Code security measures to vessels engaged in offshore activities, MODUs on location and to fixed and floating platforms. In addition, “when foreign-flagged ships are engaged in offshore supply or support activities on a State’s Continental Shelf, they can be covered by both, the requirements of the Maritime Security Measures and any additional requirement set by the coastal state” (International Maritime Organization, 2012).

In this particular subject a significant case is the model adopted by Brazil, which extended the application of the ISPS Code to MODUs and vessels engaged in offshore activities. By 31st July, 2009, and through national regulations with specific guidelines established by CONPORTOS, the Code (adapted) also applies to vessels doing cabotage and support operations to MODUs, according to the Direction of Ports and Coasts of the Ministry of Defence, Marine of Brazil.
Concerning security for oil platforms, the Brazilian government, under national law, launched a series of special regulations adapted from the ISPS Code, where fixed and floating platforms located in the Continental Shelf have been treated as port facilities and are required, in practice, to adopt the Maritime Security measures applied to port facilities as the appointment of a PFSO, the development of PFSA and the consequent implementation of PFSP. This facilities, as well as the MODUs on location and vessels that under international law are not required to comply with the ISPS Code requirements, do not get their certification in direct accordance with the ISPS Code; instead, they get issued a “Security Certificate” with the observation that it is only accepted in their national territory and not valid for international travel or operations at other nations, as established under NORMAM 01/DPC related to “Naval Craft Used at the Open Sea” and NORMAM 08/DPC related to “Traffic and Permanence of Naval Craft in Brazilian Jurisdictional Waters”.

Regrettably, the ISPS Code is mainly focused on terrorism and leaves up to each government to determine the extent to which PSO/PFSO/SSO shall reflect threats related to armed robbery; drug smuggling; stowaways; illegal migration; and the security of dangerous goods, into the evaluation of risks in the PSA/PFSA/SSA and their consequent implementation into the respective security plans (International Maritime Organization, 2012). However, for many countries these are threats with a much higher probability factor of occurrence than terror attacks.

Raymond & Morrien (2009), criticize that the ISPS Code was sold on the misleading premises that it would fundamentally address the threat of terrorism to the shipping industry; which according to them was not achieved, neither was this set of regulations able to support the shipping industry regarding other type of security challenges as armed robbery and traffic of humans and drugs at sea.

Certainly, the ISPS Code focuses on terrorism and leaves up to each government to determine the extent to which this instrument applies to threats related to armed robbery, drug smuggling, stowaways and illegal migration; but, the security measures established in the Code implicitly cover these areas. If there is a framework created by security measures including access control and monitoring, restricted security areas, strict control of unauthorized persons, fencing, lightening and CCTV monitoring the perimeter area of the port facility, together with intruder detection sensors, X-Ray cargo screening, boat patrolling sea waterways, combined with floating waterside barriers to protect waterborne access to docks, vessels and in general to the harbour area and, if necessary, underwater detection and monitoring with security trained divers for underwater surveillance and inspections of vessels and the docking area; these should be sufficient to keep port facilities free of drugs, weapons, stowaways and unlawful items.

---

8 EmbarcacionesEmpregadas na Navegação em Mar Aberto, in Portugese.
2.1.2 International Convention on Standards of Training, Certification and Watch keeping for Seafarers, 1978

The International Convention on Standards of Training, Certification and Watch keeping for Seafarers, 1978 (STCW Convention), is another international convention with important provisions regarding port and maritime security. It was adopted on 7 July 1978 and entered into force on 28 April 1984 is also extremely important concerning training for both, safety and security. And according to the IMO, the main purpose of this Convention is to promote safety of life and property at sea and the protection of the marine environment by establishing international standards of training, certification and watch keeping for seafarers. The Manila amendments to the STCW Convention and the Code were adopted on 25th June 2010, marking a major revision of both, the Convention and STCW Code.

The 2010 Manila Amendments include, among other things, measures to prevent fraudulent practices related to the expedition of certificates of competency and strengthen the evaluation process and new requirements related to training in modern technology such as electronic charts information systems (ECDIS) and Dynamic Positioning Systems; as well as marine environment awareness training and training in leadership and teamwork; updating of competence requirements for employees serving on board all types of tankers, including new requirements for personnel serving on liquefied gas tankers and for personnel serving on board ships operating in polar waters; and provisions to ensure that seafarers are properly trained to cope with a situation where their ship comes under attack by pirates (International Maritime Organization, 2015).

The set of regulations about training standards for seafarers contained in the Convention are reinforced by sections in the STCW Code, from which Part A is mandatory, while Part B contains recommended guidance to help contracting governments to implement the Convention. The minimum requirements of training concerning security awareness are established in Section A-VI/6, paragraph 4 of the STCW Code. The minimum standards of competence required for seagoing personnel are presented in detail in a series of tables. The measures, suggested in Part B, are non-mandatory and the examples given are intended to explain how some particular Convention requirements may be complied with. However, the recommended guidance represents a harmonized approach between IMO and other international organizations.

It is important to highlight that there are several areas of the STCW Code that overlap with some provisions of the ISM Code, as well as the ISPS Code. Adequate competence and training are areas addressed in the STCW Code, the ISM Code, and the ISPS Code. The concepts of maritime safety and security involve competent and sufficient crew/personnel for the respective vessel, port and port facility (port terminal).

The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention), as well as its Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf are other instruments to deal with terrorism and activities associated with terrorism in the Continental Shelf. The SUA Convention and the Protocol relating to Fixed Platforms Located on the Continental Shelf were adopted on March 10th 1988; and entered into force on March 1st 1992. The SUA Convention and the Protocol were revised in 2005, when the 2005 Protocol was added, after being adopted on October 14th 2005 and which entered into force on July 28th 2010. A total of 166 countries members of the IMO have ratified the SUA Convention of 1988 and 154 ratified the corresponding SUA Protocol of 1988. However, by March 20th. 2018, only 42 countries around the globe have ratified the SUA 2005 Convention, from which only 36 ratified the 2005 protocol (International Maritime Organization, 2018).

The ISPS Code is complemented by the SUA Convention and its 2005 Protocol, “providing a legal basis for the arrest, detention and extradition of terrorist in the event of a terrorist attack against shipping” as explained by Jones (2012).

In the case of Mexico, the SUA Convention 1988 and its Protocol was ratified. However, the Mexican authorities have yet to ratify the SUA Convention 2005 and Protocols 2005. This is a gap between international and national legislation that must be revised by the Mexican authorities.

2.1.4 United Nations Convention on the Law of the Sea (UNCLOS) & Port State Control

The United Nations Convention on the Law of the Sea (UNCLOS), is the comprehensive regime of law and order that regulates the oceans and seas of the world in the international jurisdiction, establishing rules for the governance of all uses of oceans and their natural resources. The Convention entered into force on 16 November 1994 and it is globally recognized as the international regime dealing with all subjects related to the law of the sea, such as delimitation, environmental control, economic and commercial activities in international waters and the settlement of disputes relating to ocean matters, among others. It encompasses 320 articles and nine annexes (United Nations, 1982).
The importance of the UNCLOS in relation to port and maritime security is associated to some of its articles dealing with Port State Control (PSC) and international criminal activities. Port State Control can be described as the exercise of the right of protection of the coastal state, as established in Article 25 of UNCLOS. The international IMO Conventions; such as SOLAS, including the ISPS Code, STCW and MARPOL 1973, as amended¹⁰ amongst others, provide the basis for carrying out inspections of foreign ships in national ports under PSC.

The primary obligation to ensure effective implementation and compliance with IMO requirements lies with the flag state, through flag state implementation, but simultaneously the concept of PSC provides a "safety net" to prevent substandard ships from entering/leaving the port (International Maritime Organization). Article 94 of UNCLOS establishes the duties of the flag State, requiring that:

"Every state shall effectively exercise its jurisdiction and control in administrative, technical and social matters over ships flying its flag". Provision 3 of this article reads as follows: “Every state shall take such measures for ships flying its flag as are necessary to ensure safety at sea with regard, inter alia, to: (b) the manning of ships, labour conditions and the training of crews [including security requirements], taking into account the applicable international instruments [ISPS Code]”. Provision 5 of this Article requires each State “to conform to generally accepted international regulations, procedures and practices and to take any steps which may be necessary to secure their observance”.

Through Resolution A.1052(27) adopted on 30 November, 2011, the IMO launched the new procedures for Port State Control (2011) that established guidelines for carrying out inspections under PSC. These guidelines were issued to update them, considering the amendments to IMO instruments, which had entered into force or become effective since the adoption of previous PSC resolutions. PSC procedures establish that vessels larger than 500 tons are subject to inspection of a valid International Ship Security Certificate (ISSC) on board, as required by the ISPS Code.

In cases where there are “clear grounds” for believing that the ship does not comply with the requirements of Part A of the ISPS Code (when inspecting security matters), further control measures shall be imposed, such as inspection, delaying or detention of the ship and restriction of operations within the port or even expulsion from the port, following the established in Regulation XI-2/9.1 (which applies to control of ships in port) and Regulation XI-2/9.2 (which applies to control measures to ensure compliance to ships intending to enter a port of another Contracting

Government and introduces a totally different concept of control that applies to security only) of the SOLAS Convention. These regulations are established in the ISPS Code, Part B through sections 4.29 - 4.46 about “Control and Compliance Measures”.

Currently there are nine (9) regional agreements about the implementation of PSC (Memoranda of Understanding, MoUs). Among these agreements is the Latin American one (Acuerdo de Viña del Mar). At present this MoU encompasses cooperation between Brazil, Chile, Colombia, Cuba, Ecuador, Guatemala, Honduras Mexico, Panama, Peru, Dominican Republic and Uruguay (Official Website of the Latin American Agreement of Viña del Mar). The Annual Report on Port State Control for the year 2016 in relation to the Latin American Agreement reveals that the highest number of deficiencies discovered through application of PSC in the region corresponds to Brazil with 1,432; from this number 940 were rectified, equal to 65.64% success rate. According to the same source, Colombia was the State member with the highest level of success, with 81.94 % with respect to 454 of deficiencies discovered, from which 372 were rectified. In the case of Mexico, there is a rather poor level of resolution (37.65%), with 85 deficiencies discovered through PSC, from which only 32 were effectively corrected.

Another relevant article from UNCLOS and associated to port and maritime security and directly or indirectly to PSC is Article 108, dealing with Illicit traffic of narcotic drugs or psychotropic substances. This Article reads as follows:

“All States shall cooperate in the suppression of illicit traffic in narcotic drugs and psychotropic substances engaged in by ships on the high seas contrary to international conventions. Any State which has reasonable grounds for believing that a ship flying its flag is engaged in illicit traffic in narcotic drugs or psychotropic substances may request the cooperation of other States to suppress such traffic”.

This provision is especially important in the case of Mexico, due to the fact that the highest number of port security incidents during the implementation of the “transparent port security incident reporting tool”, through this research effort, involved confiscation of narcotic drugs and psychotropic substances, as presented in Paper 5.
2.2 National legislation in Mexico for port and maritime security

To understand the evolution of maritime legislation in Mexico, it is necessary to comprehend the development of the maritime transport in the country and the changes of its control among governmental institutions. Therefore, a brief introduction of the maritime realm in Mexico is presented below.

2.2.1 Evolution of the maritime realm in Mexico

Mexico has experienced a period of extreme violence during last decades when “extortion payments” by Port Directors, concessionaries and port terminals operators to members of the organized crime to avoid damage to their installations, started, as denounced by the Federal Deputy from the Deputy Chamber of the Federal Congress, LXII Legislature, Germán Pacheco Díaz, before the National Parliament, Chamber of Deputies on 5th of November, 2013, (Cámara de Diputados del Honorable Congreso de la Unión, LXII Legislatura, 2013).

This resulted in the reorganization of maritime and port security in the country, reforms to several laws and the approval of new regulations since 2014, including the Law of Ports\textsuperscript{10}, the regulation of the CUMAR and the Law of Navigation and Maritime Trade\textsuperscript{11}, amongst others. Additionally, the creation of the UNAPROP(s) was decided. Later, on 3rd March, 2016 the President of Mexico, Enrique Peña Nieto presented a legislative initiative to reform, add and derogate diverse provisions of the Organic Law of the Federal Public Administration\textsuperscript{12}, Law of Navigation and Maritime Trade and the Law of Ports to transfer the control, inspection, vigilance and other activities related to the merchant marine and the maritime industry, including Harbour Masters and the National Maritime Authority from a civil authority (SCT) towards a military one (SEMAR), but excluding port development and its administration. This legislative initiative was approved by the National Congress without any change and published as a decree on the Official Diary of the Federation and called DOF here thereafter\textsuperscript{13} on 19th December, 2016. The decree establishes the new attributions of SEMAR, which entered into force on 17th June, 2017.

The then President “Don Porfirio Díaz” (1876-1911), instigated the development of the maritime industry in Mexico with the construction of ports as Veracruz,

\textsuperscript{10} Ley de Puertos, in Spanish.
\textsuperscript{11} Ley de Navegación y Comercio Marítimos, in Spanish.
\textsuperscript{12} Ley Orgánica de la Administración Pública Federal, in Spanish.
\textsuperscript{13} Diario Oficial de la Federación, in Spanish and represented with the acronym DOF.
Tampico, Coatzacoalcos, Manzanillo and Salina Cruz, as explained in a chronicle written by the National Congress about the development of the Mexican Merchant Marine. The maritime economic vision of Porfirio Diaz was truncated with the Mexican Revolution and recommenced during the government of General Manuel Avila Camacho, with the creation of the SEMAR, in 1940. During the government of Adolfo Ruiz Cortinez together with Rodolfo Sánchez Taboada, as the Secretary of SEMAR, started the first maritime industrial program, called “Towards the Sea”, which had the goal of the integration of a national maritime and port network; exploit the maritime resources; transfer population from the cities to the coast; establish shipyards and finally; develop the merchant marine.

According to historical records, until 1976 the SEMAR kept control of ports and the merchant marine; but in 1977 the then President José López Portillo (1976-1982) reformed the Organic Law of the Federal Public Administration, allocating to the SCT all activities related to the development and promotion of merchant marine, as well as the construction of port infrastructure and its respective administration and operation, including port and maritime security. As a part of this reform, it was also integrated into the SCT the National Commission for Coordination of Ports, the escrow for port and maritime equipment; the port services enterprises, the escrow for the Nautical Merchant School and the pilot service. It is also necessary to highlight that Lopez Portillo consolidated the tanker fleet and established the four biggest shipyards in the country: Veracruz, Mazatlán, Guaymas and Ensenada.

However, naval crafts, including patrol vessels, helicopters and other associated equipment were left to the Navy (SEMAR). SCT and particularly the Harbour Masters, never received the necessary human and material resources to exercise its authority in a satisfactory manner regarding its functions and duties related to maritime safety and security, port state control and inspection of vessels, port facilities and port terminals. In 2017, almost 40 years later, these functions were reallocated to the authorities of the SEMAR.

### 2.2.2 Port & maritime security legislation in Mexico

The IMO communicates via its web site the information that 35 different countries located in the American Continent have signed and ratified the International Convention for the Safety of Life at Sea (SOLAS), 1974; Mexico is included in the aforementioned group. Thus, Mexico, as Contracting Government to the SOLAS 1974 Convention, which includes Chapter XI-2 concerning special measures to enhance maritime security, and Regulation XI-2/3 that enshrines the International Ship and Port Facilities Security Code (ISPS Code), must fully enact the ISPS Code into national legislation.
The ISPS Code was implemented by Mexico since it entered into force in July 2004. Later it was integrated into national law through the Regulation of the CUMAR, which was published in the DOF on April 21st 2014 and is comprised of 21 articles. Its object is to regulate the organization and operation of the CUMAR, which is responsible for implementation and compliance of the ISPS Code.

The ISPS Code applies to 16 Federal Integrated Port Administrations (FIPA) in Mexico, which operate under concessions given by the SCT and are the following: Altamira, Tampico, Tuxpan, Veracruz, Coatzacoalcos, Dos Bocas, Progreso, Ensenada, Guaymas, Topolobampo, Mazatlán, Puerto Vallarta, Manzanillo, Lázaro Cárdenas, Salina Cruz y Puerto Madero, (Secretariat of Communications and Transport, 2016).

As explained before, there are three different security levels: Security Level 1 (normal); Security Level 2, (which requires additional protective security measures for a specific period of time) and; Security Level 3, (which requires specific protective security measures). In Mexico, it is the CUMAR which is responsible to ensure implementation and compliance of the ISPS Code at all security levels, as established in the Law of Ports, Article 19 TER and is responsible for decision-making, coordination and execution of all security operations under Security Level 3. The commander of the Naval Military Zone (from SEMAR) of each jurisdiction where a CUMAR is established, shall be appointed as the Chairman of that respective CUMAR, as established in provision 8 of the CUMAR’s Regulation published on the DOF on 21st April, 2014. This provision adds that the Harbour Master (which now belongs to SEMAR), shall be nominated as the Vice-Chairman of the CUMAR, plus three employees of each of these institutions, who shall be selected as advisers. A CUMAR shall be established at each of the 16 ports (FIPAs) designed to receive vessels of over 500 gross tonnage or receiving vessels trading in international traffic, according to Provision 6 of the referred regulation.

Contrariwise, the Law of Ports Article 19 BIS, establishes that the CUMAR is a group of inter institutional coordination between the SEMAR and the SCT for the application and compliance of the ISPS Code. However, since the Harbour Master’s authority figure has been transferred from SCT to SEMAR, the application of this “inter institutional character” must be reassessed, as discussed in Paper 4 of this dissertation. Article 19 TER, paragraph II of this law highlights that “the CUMAR shall apply all the dispositions and response measures within the framework of the Chapter XI-2 of the SOLAS 1974 Convention, comprising the ISPS Code and ensure the establishment of a series of functions and actions for each of the respective three security levels”. This is part of the maritime security reforms that took effect on April 21st 2014. But because of lack of knowledge about the reform itself, the SEMAR did not fully exercise its authority and the Harbour Masters, which under this reform relinquishes the chairmanship of this operative organ to the Commander
of the Navy Military Zone from SEMAR, were still erroneously recognized as the authority by PFSOs and port agencies until 2017. The CUMAR is responsible for the revision and approval of the PSA and PFSA, which covers the security risks evaluation for ports or port facilities, which shall be the base for developing the PSP or PFSP, which then, shall be submitted for revision and approval to the CUMAR. Once the Plan is approved, the Designated Authority (SEMAR from June 2017 and SCT before that) must verify its implementation and compliance through the CUMAR and issue the Statement of Compliance (SOC), which shall not exceed five years.

The responsible person for developing the PSA/PFSA and PSP/PFSP is the PSO or PFSO, including compliance of all requirements established in the ISPS Code and reflected in the PSP/PFSP as training, exercises, practices, inspections audits and modifications via formalised procedures to the plan.

As established in Paper 3, PSO/PFSO must attend security incidents and keep incident security records updated, which must be considered in the risk evaluation and integrated into the security plan to achieve a constant reduction of risks and the continuous improvement of port and maritime security. The CUMAR shall verify among other aspects, that security incidents are properly recorded in the security incidents register and even if it is the UNICAPAM (Unit of Harbour Masters and Maritime Affairs)\(^\text{14}\) from SEMAR, the responsible institution for the issuance of certification of security plans, the CUMAR is responsible for its approval and the organ that must instruct to UNICAPAM (after the last maritime reform) the issuance of the respective certificate. This, due to the established in the Law of Ports, Article 19 TER, which as explained before, says that the CUMAR is the responsible for control and compliance of the ISPS Code and co-responsible for the revision and approval of PSA/PFSA and PSP/PFSP, according to its Regulation, Article 7, paragraph II, which reads as follows:

“[CUMAR] shall participate in the evaluation of risks of maritime and port security, previous to the elaboration of the security plans and it shall propose the necessary modifications and updating to those plans”. Paragraph III of this article, adds that, once the plan has been approved, the CUMAR shall participate in the verification and control of compliance of plans ensuring its effective implementation.

This means, from a strict judicial perspective, that all current certificates of approved PSP and PFSP and even Ship Security Plans (SSP) not originally approved by the CUMAR and issued directly by the SCT were not issued in accordance to the juridical procedures. As mentioned before, the CUMAR representatives did not

---

\(^{14}\) Unidad de Capitanías de Puerto y Asuntos Marítimos, in Spanish and represented with the acronym UNICAPAM.
understand their duties and responsibilities, which were practically ignored and most PSA/PFSA and PSP/PFSP were approved directly by FIDENA\textsuperscript{15} and the certificates issued by the previous National Maritime Authority, SCT, without following the established legal procedures concerning approval by the CUMAR. The SCT renewed an agreement with FIDENA on 7\textsuperscript{th} March, 2013, to practically allow them operate as a Recognized Security Organization (RSO) and delegate some functions of the Designated Authority, including the revision and approval of PSA and PFSA, as well as the audits and verification of its implementation, without taking into consideration the established in the Law of Ports and the Regulation of the CUMAR, concerning the responsibilities of the CUMAR. Moreover, the validity of this agreement between the SCT and FIDENA can also be questionable, since the Organic Law of the Federal Public Administration, Article 16, third paragraph, establishes that “the agreements through which attributions are delegated to other administrative organs must be published in the DOF”. This agreement, which has a hypothetical validity of six years and expires in 2019, was never published in the DOF.

Therefore, the validity of Statements of Compliance of Mexican Ports should be revised concerning the issuance’s procedures, under a strict juridical perspective. Unfortunately, the majority of ports and terminals in Mexico are facing this situation. Vessels calling to ports that do not hold a valid SOC should not be able to call to American or European ports, due to their strict regulations. However, since the legality of such SOCs and ISSCs has not been evaluated yet, there has not been recorded any problem in respect of Mexican vessels calling on American ports or the case were American or European ports denied entrance to vessels that have previously conducted loading and unloading operations at Mexican ports.

Vessels that do not hold a valid ISSC or that report in the Advance Notice of Arrival (ANA form) or Advance Notice of Arrival and Departure (ANAD form, for the United States of America) to have previously performed operations at ports or terminals that do not comply with the ISPS Code, may be denied entrance to ports and port facilities that fully comply with the ISPS Code requirements, through PSC inspections for that particular port. The last 10 calls at port facilities at which the ship conducted a ship-port interface must be reported in the ANA/ANAD when vessels attempt to call a port.

Consequently, the implementation of a national program for recertification of compliance with the ISPS Code at Mexican ports and vessels to which this

\textsuperscript{15} Fideicomiso de Formación y Capacitación para el Personal de la Marina Mercante Nacional, in Spanish, in Mexico (Fund of Education and Training for the National Merchant Marine, in English, own translation).
international regulation applies is critically urgent, to avoid possible and severe international and economic consequences.

Accordingly with the CUMAR’s regulation and until this law provisions change, SEMAR must instruct the CUMARs to perform an extensive revision and approval of PSA/PFSA and PSP/PFSP at all ports in the country, and instruct/advise to UNICAPAM the issuance of the respective certificates and SOCs, and do it properly according to current procedures established by law.

2.2.3 The maritime reform of 2017 that transferred Harbour Masters from SCT to SEMAR

This legislative initiative was presented on 3rd March, 2016, by the current President of Mexico, Enrique Peña Nieto before the Chamber of Senators of the National Congress to reform the country’s legal framework and allow the shift of maritime safety and security responsibility, as well as port state control from a civil authority (SCT) towards a military one (SEMAR). Additionally, to improve the level of maritime safety and security at sea at all ports, as well as in the Mexican ocean territory. It also covered the control change of all Harbour Masters, from SCT to SEMAR. It was approved by the National Congress without any change and published as a decree on the DOF on 19th December, 2016; establishing the new attributions of the SEMAR, which entered into force after 180 “natural days” of its publication in the DOF, on 17th June, 2017.

As described in Paper 4 of this dissertation, the initiative emphasized the convenience of defining one National Maritime Authority to be able to comply with the national and international obligations, and the need to limit and redistribute the attributions that both SEMAR and SCT actually exercise. However, after the reform, several duties and responsibilities are shared and the amendments do not specify clearly enough the change from SCT to SEMAR, creating a duality of some serious attributions concerning the existence of only one entity to represent the country before international organizations for the negotiations of international treaties, and executing its obligations derived of such international conventions. Whereas SEMAR is the “Maritime National Authority” concerning maritime safety and security; SCT was also appointed as the “Maritime National Authority” for ports and its economic development. Additionally, it is attributed to SCT the “port authority”.

The legislative initiative stressed that the SEMAR as an institution of the Federal Public Administration currently has the human and material resources necessary to comply amongst other attributions, with the exercise of the national sovereignty and authority in the Mexican marine zones; guarantee the compliance of the port and maritime national legal framework; protect the maritime and fluvial traffic;
intervene in the prevention and control of marine pollution; and safeguard human life at sea, “without prejudice of the attributions that correspond to SCT in the area of merchant marine”.

The initiative, which was approved without any change, has several ambiguities. The reform to the Law of Navigation and Maritime Trade empowers both, the SEMAR and the SCT to represent the country in the negotiations with international conventions in the maritime realm; and to be the executor organ and its interpreter in the administrative sphere with respect to the attributions that according to this law, to each of them corresponds. It précises that Harbour Masters are transferred to SEMAR, redistributing the attributions that they currently have, leaving uniquely to SCT those related with the regulation, organization and administration of the merchant marine and economic administration and development of ports.

In summary, the reform provides attributions to SEMAR to approve and issue the licenses for passenger & tourism maritime transport services with small boats; authorize the vessels to bear away and bear off as well as customs clearance; flag and register of vessels, administrate the national registers both, of maritime crew and ships; inspect and verify national and foreign vessels; the compliance of international conventions as well as national legislation and official Mexican norms related to maritime safety and security; safeguard human life at sea and the prevention of marine pollution; the imposition of sanctions; as well as appointing and removing Harbour Masters. Whereas it confirms SCT to continue leading the administration of ports, stimulate port development, training and control of merchant marine; construction of port infrastructure and ocean dredging, maritime and fluvial passages; development of the maritime industry; concessions, permissions and maritime fees and in general, all maritime business related to productive activity generator of economic resources. Another inconsistency is that it will be the SCT which will be the responsible institution for planning, formulating and conducting the political programs for the development of water transport and the merchant marine and which will regulate and verify that the pilot service is offered in a safe and efficient form. The pilot service is an important part of maritime safety and security; often, it is the pilot as the first person on board who can determine if the vessel represents a risk for safety/security of ports. Currently in Mexico vessel inspections are performed at the dock in the ports, while it is recommended to carry this activity in the 12 to 24 mile Contiguous Zone. With the reform, the resources of SEMAR can allow Harbour Masters to comply with their obligations as established by law.

The reform modifies Article 7 of the Law of Navigation and Maritime Trade and establishes that the “National Maritime Authority” is exercised by the Federal Executive Power through SEMAR for the exercise of national sovereignty; maritime safety and security; as well as the Right of the State to be applied in the
marine Mexican zones; all this without prejudice to the attributions that correspond to other institutions. Concerning areas related to the merchant marine, the authorities are:

I. "Both, the SCT and the SEMAR according to their respective attributions;
II. Master Mariners of Mexican vessels; and
III. The Mexican consul abroad, authorized at the port or place where the vessel that requires the authority intervention is required for the effect that the referred law determines”.

Supporting this provision, the law decree reforms Article 8 of the Law of Navigation and Maritime Trade establishing the new attributions of the SCT, without prejudice of other institutions that belong to the Federal Public Administration. These attributions are:

I. "To plan, formulate and conduct policies and programs for the development of water transport of the merchant marine and national ports respecting the provisions established in this law and other juridical provisions applicable;
II. To represent the country in the negotiations in international treaties in the maritime domain respecting the attributions that conforming to this law corresponds, being the executor of them and its interpreter in the administrative sphere;
III. To keep the Maritime National Public Register;
IV. To integrate the statistical information of the maritime merchant transport;
V. To grant permissions and authorization of navigation to offer services in the general passages of water communication, as well as verifying its compliance, revocation or suspension of them if necessary, in the case of major naval craft;
VI. To organize, regulate and offer services of control of navigation at the ports and anchoring area.
VII. To regulate and oversee that the pilot service is offered both safely and efficiently and according to this Law and its Regulation;
VIII. To organize, promote and regulate the education and training of marine merchant’s personnel, as well as granting certificates of competence in the terms of this law and its regulation, vigil its compliance and revoke or suspend them, in cases when necessary;
IX. Participate with the SEMAR in safety of navigation and safeguard human life at sea;
X. Establish in coordination with SEMAR, the port security measures that must apply the CUMAR, conforming to the settled in the Law of Ports;
XI. Establish terms and regulations for the fees of maritime services in national territory including coastal and fluvial waters, when in the opinion of the
Federal Commission of Economic Competition, where conditions for an effective competition do not exist.

XII. To apply for the intervention of the Secretariat of Economy, when assuming the existence of international commercial practices breaching the national legislation with respect to foreign trade as well as international treaties;

XIII. To apply for the intervention of the Federal Commission of Economic Competition, when assuming the existence of practices that breach the Federal Law of Economic Competition, as well as assisting in the respective investigation;

XIV. To impose sanctions for breaches to this law and its regulations and current international treaties in the areas that correspond to this order;

XV. Other provisions from other laws and regulations juridical applicable”.

The decree also reforms Article 8 BIS of the referred Law to establish the new attributions of the SEMAR, without prejudice of other institutions that belong to the Federal Public Administration. These attributions are:

I. "To flag and register the Mexican vessels and naval artefacts;

II. Certify navigation days, issue the sea ledgers and identify the maritime personnel sailing of the Mexican merchant marine;

III. Oversee that the general communication of water passages and navigation comply with the safety conditions and maritime signalling;

IV. Oversee the safety of navigation and safeguard human life at sea;

V. Organise, regulate and, if necessary, offer services to help the navigation and maritime radio communication;

VI. Inspect and certify the Mexican vessels for compliance with the international treaties, national legislation, regulations and other Mexican norms in the area of safety navigation and human life at sea as prevention of marine pollution from ships;

VII. Inspect foreign vessels and naval craft, conforming to the established in international treaties;

VIII. Grant authorisation of inspectors as physical persons to perform the verification and certification of compliance of international treaties and the applicable national legislation, keeping supervision over such persons;

IX. Establish and organize a body of vigilance, safety and help for the navigation in fluvial waters;

X. Carry out investigations and proceedings as well as designing experts professionally empowered in the area and terms of the respective regulation to emit dictates concerning maritime and fluvial accidents and incidents;

XI. Help in the boundaries of competence with the labour authority for the compliance of resolutions maritime conflicts of labour nature;

XII. Impose sanctions for breaches to this Law and its Regulation, as well as current international treaties in the terms corresponding to this provision;
XIII. Appoint and remove Harbour Masters;
XIV. Establish and coordinate with the SCT, the maritime security measures that shall apply the CUMAR, conforming to the established in the Law of Ports;
XV. Direct, organize and carry out the search and rescue for safeguard of human life at sea in the maritime Mexican zones, as well as coordinating help and rescue in the case of accidents and incidents of vessels and port installations;
XVI. Integrate the statistical information of accidents in the marine Mexican zones;
XVII. Administrate the national registers of sea crew and vessels, conforming to the established in the respective regulation;
XVIII. Represent the country in the negotiations of international treaties in the maritime area, with respect to the attributions that conforming to this Law correspond; and being the executor organ of such treaties and its interpreter in the administrative sphere;
XIX. Other provisions from other laws and regulations juridical applicable”.

Concerning Fraction XIV of this Article, it is important to recall that according to the Law of Ports Article 19 BIS, the CUMAR is a group of inter institutional coordination between SEMAR and SCT. This part was not amended with the reform. However, since SEMAR will have the control of both, Harbour Masters and the CUMAR itself; the “inter institutional character” of this group should be re-evaluated to analyse to which extent the inter institutional coordination is necessary.

As described in Paper 4 of this dissertation, SCT kept the control of FIDENA, which in practice has some functions of a RSO. It is the authorized institution for giving the courses 18.1 (PFSO course), 18.2 (personnel with specific security duties) and 18.3 (rest of port facility personnel) concerning the ISPS Code, and in practice, since 2004, it has been the only authorized institution for performing PSA and PFSA and erroneously, performing the respective approval’s revision of PSA/PFSA, as well as inspections and audits for approval of PSP and PFSP [and also the part concerning vessels], which should had been conducted by the CUMARs. Until 2017 there was no regulation dealing with Recognized Security Organizations. Consequently, there was no RSO operating in Mexico. Because of the lack of exercise of its authority, on the part of SEMAR and the CUMARs at each port, FIDENA is also executing the annual inspections to revise compliance with PSP/PFSP.

These duties are responsibility of the CUMARs, as established in Article 12 -17 of its Regulation, where it is clear that the CUMAR is responsible for revision of PSA/PFSA and to make modifications when necessary, also to the PSP/PFSP. All these revisions, inspections and audits that should have been performed by the CUMAR and in international practice are free of charge, since these obligations provided by the National Maritime Authority, were performed and economically charged by FIDENA to port and terminal operators.
After the extensive reform of 2016, concerns have been expressed about the validity of the “inter institutional character” of the CUMAR, due to this, SCT has demanded representatives in the CUMAR. But, as discussed previously, the Regulation of the CUMAR, Article 8 establishes very clearly how it shall be constituted. The Commander of the Navy Military Zone of each jurisdiction where a CUMAR is established shall be appointed as the Chairman of that respective CUMAR, while the Harbour Master shall be nominated as the Vice-Chairman, plus three employees of each of these institutions [the Navy and the Harbour Master], who shall be selected as advisers. Currently both belong to SEMAR and therefore SCT is out of the CUMAR.

On the one hand, with the reform, the Article 8 of the CUMAR’s regulation is not harmonized with the “inter institutional character” of Article 19 of the Law of Ports. On the other hand, if they include representatives from SCT to the CUMAR, it contravenes the specifications of Article 8 of the Regulation of the CUMAR about how it shall be constituted. In both cases the constitution of the CUMAR might be declared invalid.

Yet, SCT argues that because of the inter institutional character between SCT and SEMAR, the conformation of the current CUMAR is unacceptable, while SEMAR refuses to include SCT in this organ. Therefore, in practice, the CUMAR has not been fully operating after the last reform either. To clarify these aspects, coordination between these two institutions is still necessary.

The CUMAR is currently performing the responsibilities of a Port Security Committee (PSC)\textsuperscript{16}, which is a committee recommended by the ISPS Code to coordinate security procedures and measures. Under the CUMAR is also established the Port Security Advisory Committee, which is integrated by the CUMAR, UNAPROP, customs and immigration authorities operating at the port; as well as management of the port operator and port terminals; municipal and regional authorities with interests in that specific port or jurisdiction.

The UNAPROP, which currently functions as coast guard, is under the control of the Commander of the navy zone at each port, who is the President of the CUMAR. However, as recommended in paper 4 and appended to this dissertation, the duties and responsibilities of the UNAPROP should be evaluated and confirmed. This unit currently has duties of a port and maritime police and its main function is the security of vessels (in territorial waters and those flagging the Mexican flag), ports and port facilities. According to UNAPROP’s guidelines concerning duties and responsibilities, in addition to port security; this unit is responsible for control and

\textsuperscript{16} This is also an ambiguity of IMO, which established the same acronym for both, Port Security Committee (PSC) and for Port State Control (PSC). Therefore, when referring to the Port Security Committee in this dissertation, it will be called by its full name.
compliance of the ISPS Code at the port and port terminals. But this document it’s not clear enough with respect to its duties and responsibilities under the CUMAR. The development of rules/protocols with specific and concrete duties for the UNAPROP is examined in Paper 4. The recommended duties for this unit are as follows:

- Revision and control to ensure all maritime ports and port facilities are operating with an updated and valid Statement of Compliance (SOC).
- Revision and control that all ports and terminals have employed a certified PSO/PFSO with an updated and valid certificate.
- Revision and control that all personnel from ports and terminals with security duties have been certified with the necessary training concerning the required course 18.2 as established in the ISPS Code.
- Revision and control that all personnel from ports and terminals without specific security duties have been certified with the necessary training concerning the required course 18.3 as established in the ISPS Code.
- Develop and keep the official register of maritime security incidents for that specific port.
- Revise and control that all PSO/PFSO keep updated their own register for reporting maritime security incidents.
- Participate in the revision and analysis of PSA and PFSA (for terminals).
- Participate in the inspections for approval of PSA and PFSA (for terminals).
- Participate in the revision and analysis of PSP/PFSP and make observations for necessary modifications to those plans.
- Participate in inspections and audits to verify the implementation of PSP/PFSP before the issuance of the SOC.
- Carry out random inspections onsite and general inspections to verify the compliance of PSP/PFSP during the validity period of SOCs, including the inspection areas concerning documents and records; access control; restricted area access control; availability and maintenance of security equipment; training for security equipment; handling of cargo; delivery of ship’s stores and bunkers; security procedures for monitoring security vulnerabilities acknowledged in the PSP/PFSP; procedures for threats and security incidents; security and communications; internal audits and amendments to PSP/PFSP; procedures for shore leave and visits to the ship; procedures for the interface between the ship and terminals related to ship security activities; evacuation procedures and the security procedures for protecting the PSP/PFSP from unauthorized persons and handling of
security information. All these points with specific procedures for each of the three maritime security levels (1, 2 and 3).

- Plan, coordinate and carry out security exercises (level 3) at a minimum interval of once per annum with a maximum of 18 months intervals.
- Participate in the evaluation of security exercises (level 3).
- Participate and make the necessary observation for the external security audit, which shall be performed with a minimum interval of once a year.
- Develop and keep updated the register of approved PSA/PFSA; PSP/PFSP; drills, exercises; inspections and other relevant operations for availability to IMO, in the case of mandatory audits.

The agreement number 039 was published on 31st of March, 2014 in the DOF, for the creation and activation of 19 UNAPROPs at the maritime ports of Ensenada (B.C.N.); La Paz (B.C.S.); Guaymas (Sonora); Mazatlán (Sinaloa); Puerto Vallarta (Jalisco); Manzanillo (Colima); Lazaro Cárdenas (Michoacán); Acapulco (Guerrero); Salina Cruz (Oaxaca); Puerto Chiapas (Chiapas); Matamoros, Altamira and Tampico (Tamaulipas); Tuxpan, Veracruz and Coatzacoalcos (Veracruz); Dos Bocas (Tabasco); Ciudad del Carmen (Campeche); and finally Progreso (Yucatán). However, from these 19 authorized UNAPROPs only 14 have been created and activated. It lacks its activation at the ports of La Paz, Puerto Vallarta, Matamoros and Dos Bocas. This last port also lacks the official creation of the CUMAR! This means that since the creation of the CUMAR, there has not been any authority performing port security duties and control of compliance with the ISPS Code at the Port of Dos Bocas, in which there are located some of the most important and vulnerable terminals involved with handling hydrocarbon resources.

The CUMAR and respective UNAPROP should also be created at the Federal Integrated Port Administration (FIPA) of Topolobampo and the State-owned Port Administration of Cozumel as well as at ports with Integrated Port Administrations from the National Board of Tourism17 at Cabo San Lucas and Huatulco, due to the type of operations of these ports and its importance concerning security inspections; since most of their operations are related to passenger transport and the cruise vessel industry, which could represent a target for terrorist groups.

A terror attack against a ferry that transported passengers and mainly foreigner tourists occurred on February 21st 2018, when the ferry arrived at the Cozumel port facility from Playa del Carmen, both close to Cancun (Sputnik, 2018). The referred source pointed out that the explosion left 18 persons seriously injured and that more explosives ready to be detonated were found by Federal Authorities of Mexico on March 1st in another ferry at the same port facility. The Embassy of the United States

---

17 Fondo Nacional de Turismo, and represented with the acronym FONATUR, in Spanish.
of America stated that the event was a terror attack and recommended American tourists to avoid travelling to that destination. Thus, it is recommended to extend the application of the ISPS Code to ferries of less than 500GRT sailing in main national touristic routes, which might be a target for terrorist organizations.

As mentioned in Paper 4, due to the lack of resources at the Harbour Masters offices, vessel inspections are currently performed at the dock in the ports of Mexico, which for safety and security reasons, should be done preferably outside, in the open ocean, between 12 and 24 miles in the Contiguous Zone. To allow Harbour Masters to comply with their obligations as established by law, the SEMAR should evaluate to allocate to them some of the interceptor-patrols they already have or assess the acquisition of some additional Ocean Patrol Vessel(s) Defender II, which is a relatively small naval vessel designed to perform coastal defence duties, but large and seaworthy enough to patrol offshore areas in the open ocean. Another option is to allocate interceptor patrols to the UNAPROP at least at the four hub ports of Manzanillo, Lázaro Cárdenas, Altamira and Veracruz; and also Ciudad del Carmen which encompasses the offshore area of Campeche, where the oil exploration and production zone is located; performing joint inspections between Harbour Masters and the UNAPROP, in a way that, inspectors belonging to Harbour Masters perform the verification of required certifications, and if necessary, registers, machinery, lightening, communication, and navigation equipment, anti-fire systems, life boats and marine insurances; among other aspects, while the UNAPROP may perform the inspection for issues related to the ISPS Code.

2.2.4 The decree about safety & security zones for navigation and over flight in the surroundings of offshore installations

The decree on the agreement for the establishment of safety and security zones for navigation and over flight in the surroundings of offshore installations, and integral and sustainable exploitation of fishery and aquaculture resources in Mexican marine areas, is another recently published ruling worthy to discuss. This ruling was presented by the current President of Mexico, Enrique Peña Nieto and published in the DOF on 11th October 2016. The decree has a direct impact in maritime safety and security around the oil platforms located at the Continental Shelf in the Gulf of Mexico and vessels conducting loading and unloading operations at the area.

This decree changed the provisions also established by another decree published on the DOF on 11th September 2003, where it established safety and security measures for the offshore area of Campeche. This decree established that in the “Prevention Areas” no activity would be allowed, excepting those related to oil exploration and production; but permitted the fast and uninterrupted traffic of fishery vessels en route to their fishing areas located outside the exclusion areas. The traffic of naval
vessels and aircraft entering the zones was controlled. On the other hand, it did not permit all naval traffic or aircraft, including fishing vessels, in the “Exclusion Areas”, excepting those required by the platforms. In addition the decree also required the Automatic Identification System (AIS) on board aircraft and vessels transiting in the prevention and exclusion areas already in 2003.

These provisions were derogated with the purpose of increasing the productivity of the country and reactivating the economy of those provinces, with the new decree published in the DOF on 11th October, 2016; and which entered in force already the day after its publication, on 12th October, 2016. It was decided and published without conducting any risk assessment on the impact of such decision concerning maritime safety and security. Article 1 of the new ruling established a “Security and Safety Zone” in the surroundings of oil drills, platforms and other installations for oil exploration, extraction and operation in the Mexican marine zones an area of “500 metres from its external border”; where it will only be allowed the traffic of vessels and aircraft required for the operation of such installations.

It also established a “Security and Safety Zone” of 5,500 metres in the surroundings of hydrocarbon’s export areas as the oil operation buoys or floating units for oil production, warehousing, charge and discharge; to preserve the manoeuvres of conduction, mooring, unmooring and bearing off of tankers authorized to access them; whereas the anchorage of transiting vessels not related to the activities of oil exploitation and production will only be allowed at 2,500 meters of distance from oil installations.

Article 2 of this new decree establishes that areas located outside the “Security and Safety Zone” referred to in Article 1 and where installations exist for oil exploration and extraction of hydrocarbons of submarine type; such as marine oil heads, cables or pipelines; shall not be used for anchorage, but only navigation. It adds that activities regulated in the General Law of Sustainable Fisheries and Aquaculture and other provisions deriving therefrom, can be made at a distance of 1,000 meters from these facilities, with the exception of trawling. This ruling says that only in the case of emergency when safety of human life at sea or the ship itself is in danger, will be allowed the access to these “Security and Safety Zones”, previous authorisation of that particular installation. It emphasizes that naval craft, including small vessels transiting in the surroundings of such “Security and Safety Zones”, shall have the Automatic Identification System (AIS) on board at all times, while the fishing vessels shall have the System for Localization and Monitoring of Fishing Vessels.

Article 4 of this ruling states that it will be the SCT and the SEMAR, the institutions responsible to establish the navigation rules applicable to these areas to avoid maritime accidents and incidents with the tankers that regularly operate in the zone, stressing that, “the fishing vessels shall not hinder the traffic of any tanker sailing
in the marine passages, but that it will not be forbidden to fish in the sea roadways or marine passage areas”.

Even though the UN Convention on the Law of the Sea, establishes that it shall be the coastal State member, who determines the total extension of security zones, having in mind the applicable international regulations, concerning the rule of minimum 500 metres for exclusion areas from the artificial islands and offshore installations; it is priority to make a study on how such decision will affect maritime safety and security of offshore installations and operations. Piratical acts against oil platforms located in the Gulf of Mexico increased after the security zone was reduced to 500 metres from its external border, as discussed in the next section of this dissertation.

2.3 Current security threats at Mexican ports

This part includes identified security threats to port facilities, oil terminals and oil platforms located in the Continental Shelf. Unlawful actions related to theft of hydrocarbons represent a security threat not only for the affected oil terminal, but also for the whole port facility and even for the whole community and marine environment of the port, in the case of explosions caused by such crimes. However, this risk will be assessed from a strict security perspective, including the risk of hiring personnel that passes confidential information to criminal organizations, leaving out risks connected to safety and marine environment. It is important to highlight that the Government has not been able to determine how much oil or oil products have been stolen from the different oil facilities, including port terminals. This part is based on port security incidents, which were documented in Paper 2, 3 and Paper 5.

These are the reasons and justification for one of the recommendations to the Government of Mexico discussed in Paper 4, which is to extend the application of the ISPS Code to offshore activities, including mobile offshore drilling units on location and to fixed and floating platforms by defining them as port facilities and extending all the requirements of maritime security measures required to port facilities under the ISPS Code; as the appointment of PFSO, the development of PFSA and the implementation of PFSP.

2.3.1 Security threats related to port oil terminals

Mexico faces large security challenges regarding the security of oil production, its transportation, commercialization and maritime infrastructure, even though the importance of the oil industry as the major source of income for the social
expenditure. In spite of hundreds of soldiers and navy workers, protecting the refineries, oil terminals and other important oil installations, the theft of oil products continues to increase through illegal connections to oil terminals, oil pipelines and the theft of oil tanker lorries that transport diesel and gasoline in the country.

As one of several measures to fight corruption, Mexico established in 2002 the Federal Institute of Access to the Information and Protection of Data (Instituto de Acceso a la Información y Protección de Datos, in Spanish and represented with the acronym IFAI), which in May 2012, changed name to the National Institute of Transparency, Access to the Information and Protection of Personal Data (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales in Spanish, and represented with the acronym INAI (called here thereafter with this acronym), to comply with the provisions of the new General Law of Transparency also promulgated in 2012. This law establishes that information from public institutions and all public or private persons that receive and operate money from the federal budget or national resources shall be open to the public scrutiny and the exceptions where information cannot be public to protect the national security. It also establishes that the INAI must organize the applications and send them forward to the respective institution or authority and the time limit for the delivery of information.

Exercising this right of information, an application with number 1857200255715 and dated on October 10th, 2015, was sent to the INAI to request some information from Pemex, which included several questions regarding the security and economical aspect of theft, robbery and smuggling of hydrocarbons. Among other data, it was requested statistics about tons/litres of hydrocarbons that has been stolen from oil facilities from 2000 to 2015; the number of illegal connections discovered and employees or ex-employees that had been arrested for participating in the theft of hydrocarbons; as well as the level of education and expertise of these.

On 29th October, 2015, Pemex sent the requested information by email through the INAI with the answer marked with register number SISI 1857200255715. The document only included figures for 2014 and up to October 27th 2015. However it did not include the information about the academic level of education and expertise of the employees that have been involved in theft of hydrocarbons. This was considered crucial information by the researcher since a very high level of education and training is required to make the illegal connections to pipelines and to disconnect valuable equipment from abandoned oil platforms.

As presented in Paper 2 of this dissertation, the number of legal claims and number of litres of crude oil recovered from the crime organizations for 2014 is also offered in table 1 below; while figures for the year 2015 are presented in Table 2. However, the tables do not include the amount of stolen oil not recovered by the federal police. As it can be observed in table 1 below, it is the province of Tamaulipas, where one
of the biggest oil port terminals from Pemex is located, in the Port of Tampico, which reports the highest number of theft of hydrocarbons.

Table 1
Number of litres of crude oil stolen, 2014\(^{18}\)

<table>
<thead>
<tr>
<th>Federal Entity</th>
<th>Nr. of Legal Claims</th>
<th>Nr of litres recovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mexico, DF</td>
<td>1</td>
<td>20,000</td>
</tr>
<tr>
<td>Mexico State</td>
<td>3</td>
<td>64,780</td>
</tr>
<tr>
<td>Guanajuato</td>
<td>4</td>
<td>80,000</td>
</tr>
<tr>
<td>Hidalgo</td>
<td>2</td>
<td>17,556</td>
</tr>
<tr>
<td>Jalisco</td>
<td>1</td>
<td>24</td>
</tr>
<tr>
<td>Oaxaca</td>
<td>1</td>
<td>76,702</td>
</tr>
<tr>
<td>Puebla</td>
<td>3</td>
<td>45,274</td>
</tr>
<tr>
<td>Queretaro</td>
<td>1</td>
<td>35,127</td>
</tr>
<tr>
<td>Tamaulipas</td>
<td>4</td>
<td>2,327,443</td>
</tr>
<tr>
<td>Tlaxcala</td>
<td>1</td>
<td>27,000</td>
</tr>
<tr>
<td>Veracruz</td>
<td>2</td>
<td>31,000</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>23</strong></td>
<td><strong>2,724,906</strong></td>
</tr>
</tbody>
</table>

Table 2
Number of litres of crude oil stolen 2015

<table>
<thead>
<tr>
<th>Federal Entity</th>
<th>Nr. of Legal Claims</th>
<th>Nr of litres recovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aguascalientes</td>
<td>1</td>
<td>200</td>
</tr>
<tr>
<td>Jalisco</td>
<td>1</td>
<td>57,654</td>
</tr>
<tr>
<td>Puebla</td>
<td>3</td>
<td>33,094</td>
</tr>
<tr>
<td>Tamaulipas</td>
<td>4</td>
<td>72,000</td>
</tr>
<tr>
<td>Tlaxcala</td>
<td>1</td>
<td>40,000</td>
</tr>
<tr>
<td>Veracruz</td>
<td>1</td>
<td>29,640</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>11</strong></td>
<td><strong>232,588</strong></td>
</tr>
</tbody>
</table>

The number of Pemex employees or ex-employees legally prosecuted for crimes relating theft of hydrocarbons for both 2014 and 2015 is presented in table 3, while figures of illegal connections to Pemex’s pipelines discovered and disconnected during the years 2014 and 2015 (up to October 27th 2015) are presented in Table 4.

\(^{18}\) Tables 1 and 2 were elaborated with data received from the application of information to the INAI number 1857200255715. Several of these tables are also presented in Paper 2.
Table 3
Pemex employees prosecuted for theft of hydrocarbons, 2014-2015

<table>
<thead>
<tr>
<th>Pemex’s employees or ex-employees arrested for crimes involving theft of hydrocarbons</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persons arrested and prosecuted before a Court of Justice</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Persons condemned with absolute sentence to jail</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 4
Number of illegal connections to Pemex's pipelines discovered, 2014-2015

<table>
<thead>
<tr>
<th>Illegal connections (IC) to Pemex’s pipelines discovered</th>
<th>Year</th>
<th>Quantity of Illegal Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2014</td>
<td>3,635</td>
</tr>
<tr>
<td></td>
<td>2015</td>
<td>4,298</td>
</tr>
</tbody>
</table>

In another official document with number SISI 1857200171515; Pemex informed the number of employees and ex-employees investigated for theft of hydrocarbons during the years 2006-2015; this is illustrated in Table 5.

Table 5
Number of employees/ex-employees investigated for theft of hydrocarbons per year. Period 2006-2015. Source Pemex answer to INAI, SISI 1857200171515

<table>
<thead>
<tr>
<th>Nr. of Employees and ex-employees involved and investigated in theft of hydrocarbons 2006-2015</th>
<th>Year</th>
<th>Nr. of employees investigated for theft of hydrocarbons</th>
<th>Nr. of ex-employees investigated for theft of hydrocarbons</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2006</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2007</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>2008</td>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2009</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2010</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2011</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2012</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2013</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2014</td>
<td>33</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2015</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>TOTAL</td>
<td>136</td>
<td>12</td>
<td></td>
</tr>
</tbody>
</table>

19 Table 3 and 4 are elaborated with data received from the application of information to the INAI number 1857200255715.
Table 6
Number of employees arrested theft of hydrocarbons by working division. Source Pemex’s answer to INAI, SISI 1857200171515

<table>
<thead>
<tr>
<th>Year</th>
<th>Department</th>
<th>Nr. of Employees &amp; ex-employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>Pemex Oil Refining</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>1</td>
</tr>
<tr>
<td>2007</td>
<td>Pemex Oil Refining</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td>2008</td>
<td>Pemex Oil Refining</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td>2009</td>
<td>Pemex Oil Refining</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td>2010</td>
<td>Pemex Oil Refining</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td>2011</td>
<td>Pemex Oil Refining</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td>2012</td>
<td>Pemex Oil Refining</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td>2013</td>
<td>Pemex Oil Refining</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>3</td>
</tr>
<tr>
<td>2014</td>
<td>Pemex Oil Refining</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>0</td>
</tr>
<tr>
<td>2015</td>
<td>Pemex Oil Refining</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Pemex Gas and Basic Petrochemicals</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Pemex Exploration and Production</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Pemex Petrochemicals</td>
<td>2</td>
</tr>
</tbody>
</table>

TOTAL 123

Table 6 above presents also the data of table 5, regarding number of employees and ex-employees investigated for theft of hydrocarbons during the years 2006-2015, but by division to which they were working at Pemex. Figures for other type of crimes committed by Pemex employees are presented in table 7.
Table 7
Pemex’s employees investigated for other crimes, 2006-2015

<table>
<thead>
<tr>
<th>Crime</th>
<th>Nr. of employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possession of Cocaine</td>
<td>9</td>
</tr>
<tr>
<td>Possession of Cannabis</td>
<td>25</td>
</tr>
<tr>
<td>Falsification of company’s card</td>
<td>1</td>
</tr>
<tr>
<td>Possession/bearing of fire arms</td>
<td>7</td>
</tr>
<tr>
<td>Violence with weapons</td>
<td>8</td>
</tr>
<tr>
<td>Explosion Threat</td>
<td>1</td>
</tr>
<tr>
<td>Theft of production material, ferric material, working tools, machinery, cable, pipes, car parts, cooper and cranes among other Pemex’s property items.</td>
<td>115</td>
</tr>
<tr>
<td>Murder</td>
<td>1</td>
</tr>
<tr>
<td>Kidnapping</td>
<td>2</td>
</tr>
<tr>
<td>Corruption regarding employment of staff</td>
<td>4</td>
</tr>
<tr>
<td>Improper (unmoral) Behaviour at work</td>
<td>2</td>
</tr>
<tr>
<td>Psychotropic medicine drugs</td>
<td>1</td>
</tr>
<tr>
<td>Stealing other employees properties</td>
<td>4</td>
</tr>
<tr>
<td>Falsification of fuel tickets</td>
<td>1</td>
</tr>
<tr>
<td>Car accident</td>
<td>1</td>
</tr>
<tr>
<td>Fraud</td>
<td>1</td>
</tr>
<tr>
<td>Attack/assault &amp; Violence</td>
<td>2</td>
</tr>
<tr>
<td>Being member of the “Z” narcotic organization</td>
<td>1</td>
</tr>
<tr>
<td>Alcohol at work</td>
<td>3</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>

During the period 2006-2015, 136 employees from Pemex have been investigated in relation to theft of hydrocarbons. Likewise several employees were arrested and put under investigation for other type of crimes including possession of cocaine at work installations, cannabis, and falsification of company’s card, terror attempts and murder (SISI1857200171515).

2.3.2 Criminal acts in relation to oil platforms located in the continental shelf

The definition of piracy established in UNCLOS Article 101, provides several conditions for what is to be considered piracy. These conditions include that the incident must involve violence, detention or depredation; that it must occur on the

---

20 Elaborated with information from Pemex’s answer to the INAI, SISI 1857200171515
high seas, in other words, outside the jurisdiction of any nation; that it must be following private ends (economic motives); and finally, that it must be committed on board a ship and “against a ship, aircraft, persons or property in a place outside the jurisdiction of any State”, as subsection a (ii) of the referred article reads.

Following this definition, acts of armed robbery against oil platforms located in the Continental Shelf of Mexico and within its territorial waters or national jurisdiction are not considered piracy, but unlawful acts with piratical elements. Jones (2006), criticize the UNCLOS definition and particularly the restrictive factor of the high seas, arguing that based on reports from IMO member States, most of pirate attacks take place within territorial waters or while the ship is on a berth or at anchor, which creates uncertainty about the piracy data registers might slow the juridical process against perpetrators. The referred author highlights the following definition adopted by the International Maritime Bureau (IMB) for acts of piracy:

“An act of boarding or attempting to board any ship with the intent to commit theft or any other crime and with the intent or capability to use force in the furtherance of that act”.

The IMB’s piracy definition does not restrict the pirate attack to the high seas, but on the contrary to the one established by UNCLOS, they restrict it to be against a “ship”, leaving out elements like “aircraft, persons or property” covered in the UNCLOS definition. This means that under the IMB’s definition piratical acts against an oil platform are not considered piracy either (oil rigs/platforms are not ships), even when the location factor is irrelevant and involves territorial waters.

Additionally, the piracy definition provided by the IMB does not require that the pirate attack must be committed for private ends, since it refers to theft or any crime, as opposite to the UNCLOS definition. Thus, an attack against a ship for political or terrorist motivations would not qualify as piracy under the United Nations Convention on the Law of the Sea but it would point towards that direction under the IMB’s piracy definition.

However, piratical acts against oil platforms located in the Continental Shelf are criminal activities that put in distress the security of offshore installations. The Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention), was complemented with the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, 1988, which extended the requirements of the SUA Convention to fixed platforms, as those used in the oil and gas industry for offshore operations. Its last Protocol was adopted on 14 October 2005; with entry into force on 28 July 2010 (International Maritime Organization). It is the most important international regulation concerning unlawful acts against fixed platforms offshore. However it has been critisized by several authors, as Mejia (2007) who wrote “The
Convention’s Title refers to unlawful acts but does not provide a generic character to the offenses it identifies; it ostensibly purports to combat terrorism at sea and yet fails to define it”.

Therefore it is necessary to improve the security of this type of critical infrastructure in Mexico. According to reports about security incidents and damages to marine oil platforms for the year 2016, from Pemex, and provided by one of the research participants, the number of security incidents against oil platforms increased in 2016, as presented in figures 1, 2 and 3.
Regarding the category of Robbery, it refers to equipment for the system of closing of wells, and specifically, tubing, cabling, battery banks, lifeboats and equipment to prevent or against fire. Vandalism is used when there was no robbery but only destruction of equipment and part of the installations like doors and looks; Unauthorized Access refers to the introduction of civilians without authorization to the platforms that when they see personnel from the company the intruders threat them and leave.

Besides, one of the reported incidents at the platform MANIK-A included the unauthorized access of persons armed with machete, which resulted with the few crew on board rescued by helicopters, while at platform ETKAL-101 in addition to several fire prevention equipment, a lifeboat was also stolen.

They also explained that 65 per cent of reported incidents occurred within the Tisimin Xux area and 25 per cent in the area of the oil field Cantarel, specifically 100 percent of these to the platform Akal-N. It can also be observed that 70 per cent of the incidents have occurred at satellite platforms; that 80 per cent of the incidents have occurred during the months of July (65%) and August (15%). It is also reflected that 70% of the security incidents are produced by robbery, while 30% are connected to unauthorized access of civilians at the marine platforms.

Jones (2006) classifies piracy in the following types, but specifically against vessels:

- “Opportunistic Crime (OC)
- Low Level Armed Robbery (LLAR)
- Medium Level Armed Assault and Robbery (MLAAR)
- Major Criminal Hi-jack (MCHJ)”
If Jones’s classification is applied to the type of incidents that are registered against Pemex’s oil platforms located in the Gulf of Mexico, it would be LLAR were perpetrators, considered as “simply petty criminals” use high-speed boats and weapons to board the vessel, and as long as the ship’s crew “do not act harshly, they would not be in too much danger”. Other incidents also fall in the type of MLAAR, were the “attack is often meticulously planned. Experienced seafarers and a mixture of criminal elements are often involved. They come together to form formidable pirate gangs. There is a very high risk of injury or death for innocent seafarers (...)”.

On the other hand, the type of incidents that fall in the MLAAR type are those where the lifeboat was stolen, since to launch this kind of naval craft requires a high degree of training, as well as those of stolen heliports and valuable operative equipment, which require the use of bigger craft to be transported and special expertise to be disconnected from the rest of equipment.

Illustration 4 Cuts to monitors and fire prevention equipment
The document about the incident’s report for Pemex oil platforms, specify that the possible consequences of such crimes are the following: a significant reduction in oil production caused by closing of wells; extensive damage to the marine environment caused by oil pollution, casualties and loss of life caused by over-press.

2.3.3 Security threats related to ports and port facilities in general

Diverse documented security incidents at ports and port facilities are presented and analysed in Paper 3 and Paper 5 of this dissertation. The analysis is made on the bases of the requirements and specifications of the ISPS Code, presented in section 2.1.1 of this dissertation.

The methodology for paper 3, included a questionnaire about the ISPS Code implementation, security incidents and incident reporting, sent through the INAI to Port Directors of nine different ports located in the Gulf of Mexico. However, to each of the specific questions about security incidents concerning armed attacks for robbery at the port/port facility; confiscation and smuggling of weapons and drugs or other dangerous restricted substances in the cargo; cargo theft at the port/ port facility; theft of material and other items or machinery on the part of employees, property of the port/ port facility; personnel working under the effects of drugs and psychotropic substances; situations of vandalism and sabotage; and kidnapping of port/terminal personnel, with the exception of one port, where a weapon was confiscated, the respondents from the other eight ports and Pemex terminals replied that there has never been any security incident of that nature. This significantly differs from the findings of the document analysis through Google, presented in paper 3 annexed to this dissertation.

On the other hand, security incidents and threats to ports, port facilities, oil terminals and their personnel documented in Paper 3 and 5, included transport of drugs and psychotropic material in cargo transported in vessels, which varied from the confiscation of more than eleven tons of cocaine, significant amount of weapons, confiscation of stolen crude oil transported in large tankers, kidnapping of port personnel, Armed attack against an oceanic patrol from the Mexican Navy, illegal traffic of stolen hydrocarbons, and inclusive plundering of marine oil platforms where it was stolen a whole heliport.

Furthermore, Paper 5 presents a deep analysis of security incidents documented throughout the year 2017 with the establishment of the “transparent port security incident reporting tool” developed by the researcher. The records illustrate the high risk of smuggling of weapons, drugs and illegal items.
2.4 The value of incident reporting and updating of PSA/PFSA & PSP/PFSP

The value of incident reporting and keeping updated incident security records in relation to the assessment of security threats and risks (PSA/PFSA) and its implementation to PSPs/PFSPs relies on the fact that security incident reports are the foundation for the evaluation of threats.

From this approach, if a security incident that was not considered earlier in the development of the PSA/PFSA, such assessments must be re-evaluated integrating this incident and updating security plans with the necessary amendments in accordance to the results of such re-evaluation. This is extremely valuable because it allows the continual improvement of security plans, as it should be, since ports and port facilities are subjects to constant changes and therefore the evaluation of security measures and plans must also be constant, accordingly.

As highlighted in Paper 3 of this dissertation, “the analysis of security incidents’ root causes is the cornerstone of the PFSA, which is the base of the PFSP, but if a new security threat is identified, adjustments are necessary. Therefore it is crucial to keep security incident records updated”, recalling that the ISPS Code has been designed to counter terrorism, drug smuggling, and cargo theft, among other crimes, establishing an international cooperation framework between most of the governments of the world, its government’s agencies and the shipping industry to detect security threats, as emphasized by Christopher, (2009).

As mentioned before, the IMO left to signatory governments of SOLAS the decision to extend the application of maritime security measures derived from the ISPS Code to subjects related to piracy; drug smuggling; stowaways; illegal migration; and the security of dangerous goods. However, for the case of Mexico, these types of threat have a higher factor of probability of occurrence, as presented in Paper 5 annexed to this dissertation. Under this approach these types of security incidents are included in a “transparent port security incident reporting tool”, which is also presented in paper 5, developed by the researcher and implemented at all ports in Mexico where the ISPS Code applies, by the National Maritime Authority, through UNICAPAM, from SEMAR.

This instrument included a series of incident security codes related not only to terrorism, but also to armed robbery, armed attacks against security personnel from ports and port terminals, drug smuggling; stowaways; illegal migration; unauthorized access and the security of dangerous goods among others. By applying this instrument to all Mexican ports through the official channel of SEMAR and the CUMARs and UNAPROPs at the different ports, Mexico is automatically extending the application of the ISPS Code to this type of security threats.
The application of this instrument demonstrated in a real case through “action research,” the contributions of this tool to improve incident reporting, incident investigation, PFSA and PFSP, as the ISPS Code requires. Measurements were carried out every quarter throughout the year 2017 and the incident reporting instrument was adjusted accordingly. The results show a significant improvement in reporting security incidents in the country, increasing from zero to 57, some of them considered very serious, during the first year of this tool implementation. In addition, 56% of the reported maritime incidents were associated with recommendations to be integrated into the PFSA and to be considered for improvement of PFSP.

Furthermore, the use of this tool provided PFSO with accurate information and evidence material from security incidents, which facilitated the re-evaluation of threats; proving that reporting security incidents is the key not only for re-assessment of PFSA and modifications to PFSP but also for effective incident investigation and strengthening of port security awareness.

2.5 Summary

The ISPS Code represents a structural change in port and maritime security management and should be seen as a basic framework for port and maritime security, and international cooperation, covering specific standardised security measures. Unfortunately and despite the increase of terrorist attacks and piracy, the implementation of a “security culture”, including implementation and compliance of the ISPS Code has not yet reached the level achieved by the institutionalisation, application and operation of the “safety culture” in the shipping industry. It is also important to note that security is closely related to safety; a serious security incident would put at risk the safety of the whole port, its infrastructure and personnel.

Certain SOLAS Contracting States will need to make further regulations, related to the implementation of the ISPS Code for port and maritime security, giving special focus to security challenges that affect most their territory, like armed robbery to port and port terminals; drug smuggling; and illegal migration, for the case of Mexico.

Other Contracting States, including Mexico, will have to make further regulations and a deeper risk evaluation of the threats threatening their territorial waters and other maritime installations, concerning subjects related to armed robbery on offshore installations, theft of hydrocarbons, and illegal transport of stolen hydrocarbons.
Contracting States are free to extend all or some of the ISPS Code requirements to other type of vessels than those SOLAS-class ships and port facilities addressed by the Code; and to impose greater security measures on vessels and port facilities concerning traffic of drugs and people, but respecting the provisions of other international treaties. The authorities cannot carry this out unilaterally. Governments need to involve not only the shipping industry, but all stakeholders involved, including seamen and crew organizations in order to help them understand that port and maritime security is a responsibility of everyone involved in the maritime realm, including, ship owners, crews, port administration, port terminal operators, its whole personnel, service providers, customers and even the society of the communities in which they are operating, which may contribute by informing port security authorities of suspect items or activities around the port.

The integration of everyone in the process of strengthening port and maritime security will ensure continuous, effective and satisfactory commercial operations. Authorities from neighbouring countries could also be involved in this process to strengthen an open international cooperation neutralizing the fear of violence of sovereignty rights for the States, especially in consideration that terror actions against offshore and port facilities located close to the border lines may result in extensive environmental and economic damage for both nations.

Yet, it may be argued that an international harmonisation of the implementation of the Code is desired to ensure international cooperation between Contracting States; in that case States will be free to enforce greater security measures than those established in the ISPS Code, if the protection of port facilities and sea waters in their country requires that. In this process, they must also procure efficient and continuous commercial operations at ports, and respect the provisions of other applicable international treaties, for example those that are protected by diplomatic principles. It is important to stress that this international set of regulations allows for differences in the implementation and compliance regarding the implementation of greater security measures than those established in the ISPS Code, but not less. This is to ensure the harmonisation of the rules to the minimum level established by the Code.

Finally, the main instruments and key concepts related to port and maritime security are addressed in the ISPS Code. If these are efficiently implemented according to the principles, provisions and guidelines established by the same Code; its compliance is verified systematically; and they are updated in accordance with new security threats, they are good enough to ensure the security of port facilities, vessels and territorial sea waters, to an acceptable risk level.
3. Research objectives

As stated in the introduction, the aim of this dissertation is to contribute to the maritime world by developing an instrument that can be used to set up the strategies at a macro level for building a national maritime security policy in any Contracting State to the SOLAS Convention around the globe, and at the same time improve security incident reporting and incident investigation. The development of this instrument is under the context of the maritime and particularly, port security situation of Mexico, but with application to other regions of the world facing similar security threats, as smuggling of drugs and weapons, illegal goods, theft of hydrocarbons, dissemination of port security classified information, unauthorized persons in port and seaways restricted areas, and misuse of access identity cards, among others.

As a part of this, another aim of this research effort is to study the current situation of maritime security and particularly port security in Mexico, including a critical analysis of the national legal framework for port and maritime security related to the enactment of the ISPS Code into national legislation in Mexico; as well as the current security threats at Mexican ports and port facilities. Additionally, this research intends to contribute to the understanding of the value of reporting security incidents, and updating of security incident logs, by taking into consideration those security incidents classified as “serious,” results of security drills and exercises for reassessment of PFSA/PSA, with the consequent amendments to PFSP/PSP. It is important to recall that such changes must be tested and updated accordingly to manage security threats and maintain the security of the port at an acceptable level. This, to develop an analytical transparent incident-reporting tool useful not only for updating of Port Facility Security Assessments and respective Security Plans, but also, to provide official security incidents investigators with all the necessary information to investigate the event and instruct the implementation of measures that could prevent the re-occurrence of such incident. This Instrument can also be used to establish the necessary strategies to develop a national maritime security policy. The goal is also to implement this instrument in Mexico, helping the State to improve maritime and in particular port security, testing it through action research and improving it in the process, to finally offer it to other regions of the world that might benefit from it.
As Mejia (2007) pointed out, “one of the many challenges facing policy makers is the lack of useful tools for the multilevel analysis of the security seascape [port facilities in our case] to facilitate the identification of problem areas and the formulation of appropriate, perhaps even proactive, actions plans”. The author referred to Schröder (2005) to highlight the paucity in tools available for assessing and managing risk in maritime security. It is important to recall that under his approach maritime security covers port security, which means the extension of the problem to the port security area as well. Currently, the tools used in port security are developed for application at an operational level for port facilities and not at a national level. This tool will provide the State with crucial information at a macro level that can be used to set up the strategy for developing a national maritime security policy.

Based on these goals, the general research objectives are developed and presented in this section with the specific objectives of each of the annexed papers.

### 3.1 General research objectives

As mentioned previously, this doctoral dissertation intends to contribute to improving maritime and port security worldwide by developing an instrument useful to set up the strategies to build a national maritime security policy. To do this, it is a prerequisite to understand the legal framework of the State where it will be implemented, as well as security threats for that particular Nation; Mexico, in this case, studying the level of compliance with the ISPS Code by the Mexican government, both from a legal and practical perspective.

From the legal perspective, it attempts to identify the legal gaps between international and national legislation in relation to the enactment of the ISPS Code, and its harmonization in national law to allow full compliance from all actors involved.

From the practical perspective, it strives to identify threats to port security, including oil terminals as well as oil platforms; improve the development of PSA/PFSA AND PSP/PFSP, increasing the focus on security incident-reporting and security incident investigation by extending the application of the ISPS Code to both:

1) MODUs on location, fixed and floating oil platforms through the development of national regulations by defining these type of offshore installations as “port facilities” to be covered by the requirements of the ISPS Code regarding the appointment of a PFSO, the development of PFSA and the implementation of PFSP and;
2) Subjects concerning drug smuggling; stowaways; illegal migration; and other serious security threats not directly covered by this set of regulations.

The identification of security threats is necessary to develop an analytical transparent incident-reporting tool suitable to support security incident reporting, improve PFSA and PFSP and port/maritime security incident investigation. To create an instrument that would also be useful to set up strategies for building and implementation of a national maritime security policy. This innovative instrument will be tested through action research in Mexico, with the support of the Mexican Government. Action research will allow to discover the strengths and weaknesses of this tool and improve it during the testing period (2017), through its application in a real case.

This is intended to be achieved by pursuing the subsequent general objectives:

3.1.1 Elaborate a critical analysis of the current port security situation of Mexico, with special focus on implementation and compliance of the ISPS Code, including the state of the art and harmonization of international legislation with national law.

This objective is first, to study the state of the art related to the implementation and compliance of the ISPS Code within the context of port security and oil terminals in Mexico, covering the need of understanding the fundamentals and evolution of the topic to set up the theoretical framework for this research effort. Secondly, to establish the directions of the study, it’s priority to critically analyse the enactment of the ISPS Code into national law in Mexico; understanding the strengths and deficiencies of the port and maritime security legal framework of the referred country in relation to Chapter XI-2 of the Safety of Life at Sea Convention 1974, (SOLAS Convention), covering the need to understand the legal framework, from a strict juridical perspective, that establishes the bases for compliance of the ISPS Code in this Contracting State. Additionally, elaborating a critical evaluation of the level of implementation and compliance of the ISPS Code, by the Mexican government, with focus on port facilities from a practical perspective, covers the need to find the deficiencies and areas of opportunity for improvement including security incident reporting and incident investigation.

3.1.2 Identify the most relevant security threats to port facilities in Mexico, including oil terminals, and offshore installations

This objective will cover the need to discover the most relevant security threats at ports and port facilities in Mexico to study them in relation to the reported security incidents. Identifying security threats and areas that can represent a security risk for
the port facility, its whole infrastructure, personnel, customers and in general, all persons involved with the port operations is necessary to develop the analytical transparent incident-reporting tool. Identification of security threats is also essential to implement security measures, plan for security incident response and be able to mitigate its consequences.

3.1.3 Develop an analytical instrument for security incidents-reporting & incident investigation, to strengthen the continual evolution of PSA/PFSA and PSP/PFSP and useful for setting up the strategies of a national maritime security policy

The third general objective of this dissertation is to develop an analytical transparent incident-reporting tool to support security incident reporting and incident investigation, which simultaneously is useful to establish the strategies to build a national maritime security policy. This is intended to be done, by acquiring all relevant information of a particular event in this security incident-reporting tool, thereby facilitating a learning process from that particular security incident and use it not only for updating of PSA/PFSA and respective PSP/PFSP, but also, to provide official security incidents investigators with all the necessary information to investigate the event and instruct the implementation of measures that could prevent the re-occurrence of such event. Moreover, acquiring all data related to all security incidents at all ports and port facilities across the country would provide the State with crucial information at a macro level useful to set up the strategies, including allocation of material, economic and human resources, which would be the foundation for developing a national maritime security policy.

3.2 Objectives of the individual papers

This doctoral dissertation incorporates five articles. Two of these have been published as book chapters, two more were published in an international journal, and another one has been accepted for publication and is currently in press. The objectives for each of these papers are presented below:

The objective of this paper is to examine the state of the art related to the implementation and compliance of the ISPS Code, within the context of port security in Mexico, based on a cross-disciplinary approach among eight selected categories.

**Paper 2**  

The objective of paper 2 is to review the situation of the oil industry from a strict security perspective and discuss key elements of port and maritime security; addressing the necessity of the inclusion of port and maritime security and the protection of critical oil infrastructure located in the Continental Shelf in the national agenda, which would provide for future research directions in the maritime security domain and contribute to the establishment of a national maritime security policy.

**Paper 3**  

The objective of paper 3 is to examine three different options/solutions that Mexico implemented within its ports and offshore installations in order to improve the country’s maritime security situation, as well as ensuring compliance with the ISPS Code: privatization, militarization and finally, their combination.

**Paper 4**  

The objective of paper 4 is to examine the latest maritime reform in Mexico, which provides the legal framework to shift the National Maritime Authority from a civil institution (SCT), towards a military one (SEMAR). As well as its extent of harmonisation with international law in respect of the ISPS Code implementation and compliance; and the critical situation that the shipping and oil industry is facing.
Another objective of this article is to study the level of acceptance concerning the shift of the National Maritime Authority from SCT to SEMAR, between the four pillars of representatives of authorities/institutions directly related to duties and operations within these two important domains, a prerequisite for success.


The first objective of paper 5 is to develop an analytical transparent incident-reporting tool to be used to support security incident reporting, improve PFSA and PFSP and port/maritime security incident investigation. By acquiring all relevant information of a particular event in this security incident-reporting tool would facilitate learning from that particular security incident and use it not only for updating of Port Facility Security Assessments and respective Security Plans, but also, to provide official security incidents investigators with all the necessary information to investigate the event and instruct the implementation of measures that could prevent the re-occurrence of such event. The second objective of this article is to examine port security at Mexican ports from an incident reporting and investigation perspective by implementing this instrument at all ports in Mexico where the ISPS Code applies, with the support of the National Maritime Authority, demonstrating in a real case through “action research,” the contributions of this instrument to improve incident reporting, incident investigation, PFSA and PFSP, as the ISPS Code requires. The third objective of this paper, is to demonstrate the use of this tool for a multilevel analysis of port security threats to identify the problem areas and contribute to set up the strategies for the development of a national maritime security policy.
4. Materials and methods

The methodological approach adopted in this doctoral dissertation is principally based on qualitative methods, including action research with a limited use of statistics, which are mainly used in paper 5, for the development of the analytical transparent incident-reporting instrument to be used to support security incident reporting, improve PFSA and PFSP and port/maritime security incident investigation.

Based on this, it was developed a Model for Port and Maritime Security Incident Investigation. On the bases of this Model, a new and “transparent incident-reporting tool” was developed, building the bridge between PFSA, PFSP and port security incident investigation, as illustrated in the model below.

Illustration 5 Model for port and maritime security incident investigation
The selection of methods is based on their suitability in both, law and social sciences, disciplines where they are widely used, in accordance with the exploratory nature of political themes as in this case; where one of the general objectives is to contribute to the development of a national maritime security policy. These were combined in the last phase of the study with action research, which is necessary to implement, test and improve the above-referred tool.

The research objectives call for classical documental analyses examining the elements of the relevant international legislation against its implementation into national legislation in the referred nation-state. The objectives also require the use of semi-structured interviews and participant observation to identify security threats at the field study.

The questionnaires used to perform the semi-structured interviews include questions for the different papers and therefore, the same questionnaire, but different questions were used to develop the different articles annexed to this doctoral dissertation.

Structured and semi-structured questionnaires with open questions, helped the researcher to avoid being obtrusive and engaging in active listening strategies during the interview. McCracken (1988) pointed out that active listening strategies, must not be used by the qualitative researcher because they are obtrusive and likely to be almost completely destructive of good data. This can be avoided through the use of the construction of a well-designed questionnaire, which has several functions; it ensures covering all subjects in the same order for each respondent; establishes channels for the direction and scope of discourse; and allows the scientist to give all his/her attention to the informant’s testimony.

By referring to Merton, Fiske and Kendall (1956), McCracken (1988) emphasized that the use of questionnaires does not pre-empt the “open-ended” nature of the qualitative interview; because within each of the questions, the opportunity for exploratory, unstructured responses remains.

Structured questionnaires with open questions help researchers to give order to the subjects during the interviews, which simplify data analysis while developing categories or themes.

As mentioned above, during the last phase of the study, Action Research was used. It is a form of interactive inquiry process that balances problem solving, actions implemented in an interactive context with data-driven and collaborative analysis or research, allowing practitioners to evaluate their job and understand the underlying problem causes, enabling organizational change (Reason & Bradbury, 2001).

The figure following illustrates an action-reflection cycle for action research.
Illustration 6 Action-reflection cycle (Mcniff, 2011)

Figure 6 illustrates how the researcher identifies a particular subject, investigates different ways of doing their job, reflects on what is happening and why, check out any new understandings with others - and in light of those reflections - try new ways or methods to do their tasks that may or may not be more successful. If the trials show that the tested methods are better, then the individual or the group moves forward in that new direction.

Mcniff (2011) stated that Action Research is meant to be a systematic process and recommends to use this type of research when the goals of the researcher are to improve his/others understanding, develop his/others learning and influence other’s learning. He places the emphasis of the study on the researcher’s intent to take action for social improvement. This is highly relevant to the general objectives of this research study and the objectives of paper five, which are the following:

a) Develop an analytical transparent incident-reporting tool to be used to support security incident reporting, improve PFSA and PFSP and port/maritime security incident investigation;

b) Examine port security at Mexican ports from an incident reporting and investigation perspective by implementing this instrument at all ports in Mexico where the ISPS Code applies, with the support of the National Maritime Authority, testing and demonstrating in a real case the contributions of this instrument to improve incident reporting, incident investigation, PFSA and PFSP, as the ISPS Code requires.
c) Demonstrate the use of this tool for a multilevel analysis of port security threats to identify the problem areas and contribute to set up the strategies for the development of a national maritime security policy.

In accordance with these objectives, the researcher is expected to actively participate in testing the instrument and apply the necessary changes through the testing period, which in coordination with the SEMAR of Mexico, is set up to the entire year of 2017. After which, they will continue operating the instrument on their own. Due to its extent, the transparent incident-reporting tool is presented as annex to this dissertation, both in English and in Spanish.

This is the first time that an external academic institution was allowed to conduct a scientific study involving the direct participation of the Mexican Navy and Customs authorities and that results were published openly and made available for anyone. The methodological approach of “Action Research” used to test and improve the proposed transparent security-incident reporting tool required a strong interaction between the researcher and the representatives of the Mexican Navy and indirectly from Port Facility Security Officers (PFSO) at all ports in Mexico as well, during the complete testing period of the year 2017. The use of Action research in this academic effort makes this a distinctive research undertaking that provides a unique insight into port security threats, port security systems and the naval world.

The methodological approach of “Action Research” also demanded a close joint analysis of data between the researcher and the representatives of the institution (research setting). As mentioned before, data was collected every quarter through 2017 and scrutinized to analyze security incidents, with special focus on the discovery of new security threats not considered in the security incident-reporting instrument. New codes were allocated and the respective incidents were followed up. This would not have been possible without the direct participation of the Mexican Navy and the selected research methods.


Research methodology for paper 1 involved a review of the published literature on the subject. Webster & Watson (2002, p. xiv) explained that a high quality review must cover all relevant literature on the topic and should not be confined to a limited set of journals. The literature search method encompassed querying ten (10) different scientific databases as proposed by Webster & Watson (2002, p. xvi).
Apart from articles, the literature review also included book chapters and other relevant documents captured during the search process. The analysis of the relevant literature was made on the bases of eight categories. This allowed the conversion from the author-centric approach towards the category-centric approach and synthesise the relevant literature, developing a category matrix in relation to the selected categories with a cross-discipline fertilisation approach. The selected literature was then analysed with a geographical approach. After the first search, in 2015, a second search in 2018 was conducted to update data and verify the inexistence of research contributions for the specified search parameters.

4.2 Paper 2: Opening of offshore oil business in Mexico and associated framework to cope with potential security risks

The methodology for Paper 2 included documental analysis and critical review of the actual situation of port and oil terminals with special focus on the oil industry in Mexico from the security perspective. The data was gathered from different sources that included official information from Petroleos Mexicanos (Pemex), the Mexican oil agency and various authorities. In addition some very relevant information was requested from Pemex and port administrations through the National Institute of Transparency, Access to the Information and Protection of Personal Data (INAI). Once the relevant documents for this topic were gathered, they were further selected and classified according to their relevance to the study.

4.3 Paper 3: Enhancing maritime security in Mexico: Privatization, militarization, or a combination of both?

The research methodology for paper 3 included the use of an extended questionnaire with 71 open questions concerning maritime security, sent to eight (8) ports of Mexico; through the INAI. A questionnaire of 70 similar questions (but, specifically addressed to oil port terminals) was also sent to “Pemex Exploración y Producción,” through the INAI to acquire information for their port and terminals. An inquiry about the establishment of the UNAPROP at the different ports of Mexico was sent to the SEMAR, whilst another request of information about the total number of persons employed at private security companies that have got the courses 18.2 and 18.3 as required in the ISPS Code was sent to the FIDENA, also through the INAI. The INAI was created to comply with the provisions of the General Law of
Transparency promulgated in 2012. This law establishes that information from public institutions operating money from national resources shall be open to public scrutiny with exceptions related to national security.

These actions were combined with a six-day visit of the researcher in one of the three largest ports of Mexico with port oil terminals conducted in April 2016, where she performed interviews and “participant observation.” The questionnaire that was sent to the other ports through the INAI; was also answered by respondents at that specific port. At this port, the researcher participated as observer at the preparations, performance and post-evaluation of an exercise at level 3, of those required by the ISPS Code. Listening to arguments in many different directions while the preparations and execution of the exercise for security incident response and its evaluation awarded the researcher with a unique insight about deficiencies and adequate actions of the actors involves when undertaking such exercises.

The results from the questionnaire were examined using document analysis with an exploratory approach, to confirm or reject the inexistence of security incidents at the selected ports and oil terminals trough a critical review of security incidents reported in national newspapers and media sources, using Google to have a wider coverture within the period of 2004-2015.

4.4 Paper 4: Mexico's reorganisation of maritime security regime: A new role for the navy and emphasis on energy related infrastructures

The research methodology of the current study includes semi-structured interviews made to Harbours Masters, Directors of Customs Maritime Units, Port Administration Directors, PFSOs from ports and certain number of hydrocarbons terminals, Presidents of CUMAR (1st Commander of the Navy Zone, Navy Sector or Navy Station) and Commandants of the UNAPROP. Additionally, participant observation at the terminals and harbours master’s installations and ports, including not only the land areas but also the maritime passages took place; they were visited on board oceanic patrols from the Mexican Navy. The visit to the mentioned ports in Mexico had an average duration of one week at each port. The observation of normal daily operations at the different areas of the ports, including the Customs Maritime Unit installations, the oil port terminals and the navy security areas provided the researcher with a unique insight of the strengths and weaknesses of port security in México, as well as the opportunity areas for improvement, by identifying the most relevant security threats and problem areas, as well as the level of cooperation between these institutions at the ports.
The poll of data included the leaders of the mentioned institutions from the ports of Altamira and Tampico (Tamps.), Tuxpan, Veracruz and Coatzacoalcos (Ver.), Dos Bocas (Tab.), Ciudad del Carmen (Campeche); Progresso (Yuc.); as well as another Hub Port from the Pacific in Mexico. By doing this, the researcher covered the four pillars for the operation of the port. The pool of data is deemed sufficient, based on the fact that it includes eight out of sixteen FIPA in Mexico where the ISPS Code applies, representing a coverage of 50% of them and seven out of seven FIPAs situated in the Gulf of Mexico, where oil exploration and production activities take place, achieving a 100% coverage of them. One State-Owned Integrated Port Administration (Ciudad del Carmen, Campeche) where most of the oil activity is concentrated was also included in the study. Two informal interviews of top Directors from SEMAR were performed on key themes identified from issues prevalent in the analysis of the interviews to Presidents of the CUMAR and Federal FIPAs. From the total of persons invited to participate and representing Harbour Master offices at these nine cited ports, only one of them rejected the invitation. The same figures correspond to representatives from the Customs Maritime Units (one) and Directors from FIPAs (one) as well as the PFSO from that same port that due to extreme work volume had to decline the interview.

The purpose of the study was described to the participants via an information cover-sheet letter where the research objectives were explained, clarifying that their participation was voluntary, confidential and without any economic contribution, or gifts. The Research Ethics Committee of the World Maritime University approved the study. The total of interviewed participants was 57 persons, all involved in areas of maritime safety and security. The semi-structured interviews were carried out in the participant’s workplaces by the researcher and free from intervention with management and carried out during the visits to the installations for participant observation, which uncovered several aspects and deficiencies of the implementation and compliance of the ISPS Code in Mexico.

4.5 Paper 5: Integrating the procedures of reporting port security incidents and the follow-up investigation to build a national maritime security policy: A case study in Mexico

Paper 5 includes the first stage of the design, an analysis of data developed from the same semi-structured interviews with Harbour Masters, Directors of Customs Maritime Units; Port Administration Directors; PFSOs from ports and some terminals of hydrocarbons; Presidents of CUMARs (1st Commander of the Navy
Zone, Navy Sector or Navy Station) and Commandants of the UNAPROP, used for paper 4.

It uses qualitative semi-structured interviews to allow new viewpoints to emerge freely, particularly about their opinion and perception concerning port security threats. This method is valuable to study opinions and fears of people when changing processes and systems, especially after the shift of maritime safety and security responsibility, as well as port state control from SCT to SEMAR.

In a second stage of the research and after the findings of the 15 themes; “Action Research” was integrated into the methodology with the genuine interest of contributing to improve maritime security in the country. A three day ISPS Code implementation and compliance course was provided to Admirals from the CUMAR and Commanders from the UNAPROP from all ports on 17th, 18th and 22nd November 2016.

Based on the findings of the interviews and participant observation, the researchers developed a new and “transparent incident reporting tool”, as mentioned before, which was implemented at all ports in Mexico where the ISPS Code applies, by the National Maritime Authority of Mexico. The purpose of this was to test the instrument, and demonstrate in an actual case through “action research,” its contributions to improve incident reporting, incident investigation, PFSA and PFSP, as the ISPS Code requires. Measurements were carried out every quarter throughout the year 2017 and the incident-reporting instrument was adjusted accordingly when incidents without code were reported, adding new codes. As mentioned previously, due to its extent, it is annexed to this dissertation both, in English in Spanish. The Spanish version is the one implemented in México; but the English is also provided with the hope that other countries facing the same problematic might benefit from that instrument.

### 4.6 Scope & delimitations

The main scope of this research effort is to evaluate the level of implementation and compliance of the ISPS Code in Mexico, as well as identify the most relevant security threats at port facilities and port oil terminals and fixed and floating platforms in this nation State. To develop and implement the “transparent incident reporting tool” referred to above. It shall be highlighted that even if this instrument is developed tested and implemented at the different ports of Mexico were the ISPS Code applies, it can be applicable to other regions of the world facing similar security threats.
An important limitation to mention is that the research only considers ports (common areas) oil port facilities and marine oil platforms in Mexico, concerning the interviews. However the instrument for reporting of incidents was applied at all Mexican ports, including most type of port facilities.

The study focuses mainly on port security and to a limited extent, maritime security, excluding other areas like safety, economics and marine environment, since these are topics of such importance that they deserve their own study.

The doctoral dissertation is presented in the compilation format, compiling all the articles and manuscripts published by the candidate about the topic. This design was advised because through the research the referred tool and other recommendations following the published articles were implemented during the research period, and the security status is already improving, avoiding that the research loses its actuality and relevancy.

4.7 Validity and reliability

Validity has been described by Francfort-Nachmias & Nachmias (1996) as understanding the question “Am I measuring what I intend to measure?” Reliability, as Mejia (2007) explains, “It refers to the extent to which a measuring tool contains variable errors, that is, errors that appear inconsistently from observation, to observation during any single measurement attempt”.

Qualitative methods and specifically; interviews, participant observation and action research are mainly used in this study. Qualitative methods are used to describe the world of the human experience, emotions, perceptions and its interaction with groups of a specific type with defined tasks or responsibilities, among other aspects. Several researchers have criticised that qualitative methods are largely exposed to the subjective experience, disapproving its application in terms of validity and reliability. Both, qualitative and quantitative methods aim to reveal the truth about the investigated phenomena. As Bashir, Afzal, & Azeem (2008), established, the validity and norms applied to quantitative research do not completely apply to qualitative research. The referred authors wrote:

“Validity in qualitative research means the extent to which the data is plausible, credible and trustworthy; and thus can be defended when challenged. Reliability and validity remain appropriate concepts for attaining rigor in qualitative research. Qualitative researchers have to salvage responsibility for reliability and validity by implementing verification strategies integral and self-correcting during the conduct of inquiry itself. This ensures the attainment of rigor using strategies inherent within each qualitative design, and moves the responsibility for incorporating and
maintaining reliability and validity from external reviewers’ judgments to the investigators themselves”.

Even if interviews and participant observation do not score high in tests of validity and reliability, it does not necessarily mean that the methods applied are not acceptable. Stanton & MS (1998) argued that, “analysts should be aware of the potential power of the method before they use it, rather than proposing that they should not use it”.

Mejia (2007) clarified that it does not mean that validity and reliability are not essential in qualitative methods, instead, he argues “different methods are appropriate in different stages of the design and one method scores differently from the other in terms of reliability and liability”. Kvale (1995) discusses validation of qualitative research relation to postmodern conceptions of knowledge and presented three different approaches to validity:

“First, validity is treated as an expression of craftsmanship, with an emphasis on quality of research by checking, questioning, and theorizing on the nature of the phenomena investigated. Second, by going beyond correspondence criteria of validity, the emphasis on observation is extended to include conversation about the observations, with a communicative concept of validity. Third, by discarding a modern legitimation mania, justification of knowledge is replaced by application, with a pragmatic concept of validity. In conclusion, the validity of the validity question is questioned”.

Action Research is a form of interactive inquiry process that balances problem solving, actions implemented in an interactive context with data-driven and collaborative analysis or research, allowing practitioners to evaluate their job and understand the underlying problem causes, enabling organizational change (Reason & Bradbury, 2001). It is about how the researcher identifies a particular subject and undertakes alternative methods of carrying out that particular job, reflects on what is happening and why, checks out any new understandings with others involved and in light of those reflections - tries new ways or methods to do their tasks that may or may not be more successful. If the trials show that the tested methods are better, then the individual or the group moves forward in that new direction. It requires constant evaluation, judgment and trial. McNiff (2011) suggested that Action Research is meant to be a systematic process and recommended the use of this type of research when the emphasis of the study on the researcher’s intent is to take action for social improvement.

McTaggar (1998) analysed validity in participatory action research, in terms of content and outcome. He said that for participatory action, researchers report on how things changed. Because of the shared work between the participants and the researcher the focus should be on the research itself as well as it’s reporting,
including the crucial questions of “how things were changed and how things were resisted”. He adds categorically that, “validity implies content. It requires thinking about how a social practice has changed”. He proposes that the following questions must be considered in the participatory research reporting:

1. “How have things changed?
2. What has not changed?
3. What has been confirmed?
4. What has been ignored?
5. What has been made problematic”?

Each of these questions is thoroughly answered in section 6 of this dissertation, which presents the discussion and conclusions. McTaggar, (1998) argued that the use of several methods is possible in action research to achieve validation. This is known as triangulation. This coincides with Hoepfl (1997), who also wrote that triangulation may enhance validity in qualitative methods. By referring to Alison, (2005), Mejia (2007), clarifies that triangulation is acceptable under the premises that “no single approach ever really solves, delineates, or validates a particular problem. Different methodologies, investigative approaches and other types of triangulation yield more complete data and result in more credible findings”. He explains that there are four types of triangulation: a) data triangulation; b) investigative triangulation; c) theory triangulation; and d) methods triangulation. Methods triangulation is defined by Alison (2005), as “the use of different methods to study a single research problem,” according to the referred by Mejia (2007).

Methods triangulation was applied in this doctoral dissertation by using interviews (semi-structured using a questionnaire with open questions, which was approved by the Research Ethical Committee of this World Maritime University upon starting the study); heuristics (document analysis); observation (visits to eight ports of Mexico including Customs Maritime Units, port terminals, Navy Zones, Harbour Masters, oil platforms and observing patrolling of port navigation channels and the Continental Shelf with the Mexican Navy on board oceanic patrols. In addition the sea waters of Campeche and Tabasco, were most fixed and floating platforms are located, were flown by helicopter to explore the security at offshore facilities). Finally, it was also used action research for the implementation of the “transparent incident-reporting tool”.
5. Results

5.1 Paper 1: Implementation and compliance of the International Ship and Port Facility Security Code in Mexico: A literature review and selected issues

This paper provides a literature review of the state of the art on implementation and compliance of the ISPS Code for the case of Mexico. This investigation was initially oriented solely towards Mexico. Due to the absence of research within this subject for the referred country the review had to be done through subcategories with the conditional connection of Mexico and relevant issues were selected. The primary data confirmed the absence of research within this subject in Mexico. The secondary data, were other words related to the ISPS Code were used for the search, allowed for a wider geographical coverage and expanded on general bases the scope of analysis, since ten (10) different academic databases were exploited. The literature review from an author-centric approach is initially presented; then, it is used as the basis to further develop (and examine) the concept-centric approach, through eight selected categories. The careful screening of literature, constructed on specific concepts, allowed the identification of cross fertilization of such concepts in the respective fields. It is observed that the research efforts focused on the ISPS Code and the development of a PFSP have an integrated perspective, where the categories of terrorism and counterterrorism, as well as maritime security management and the issue of port security have a strong interaction and dominant status. The results demonstrate the limited number of academic contributions in these areas from America Central and South America in relation to other parts of the globe, as well as the total absence of research efforts about the ISPS Code in Mexico. In the scientific contributions on the subject were Mexico is included; it is in reference to isolated cases of armed robbery, drugs organizations or proliferation of crime on general bases, but not regarding the ISPS Code itself. The absence of scientific research on this area for the specific country might also be related to the lack of a national maritime security policy and a poor maritime security culture as the authors have pointed out in other contributions.
5.2 Paper 2: Opening of offshore oil business in Mexico and associated framework to cope with potential security threats

Paper 2 describes the situation of Mexican ports and the oil industry from a security perspective and discusses key elements of port and maritime security; addressing the necessity of the inclusion of port and maritime security and the protection of critical oil infrastructure located in the Continental Shelf in the national agenda which would provide for future research directions in the maritime security domain and contribute to the establishment of a national maritime security policy. It identifies the substantial security challenges that are facing maritime port and the oil industry in Mexico; and proves that the losses are not limited to economic factors, but also to loss of civilian life and the environment. It calls for attention of the subject of port and maritime security in the national agenda for the development of a national maritime security policy to provide the foundation for an effective and proactive port and maritime security programme.

5.3 Paper 3: Enhancing maritime security in Mexico: Privatization, militarization, or a combination of both?

Paper 3 examines three different options/solutions that Mexico implemented within its ports and offshore installations in order to improve the country’s maritime security framework, as well as ensuring compliance with the ISPS Code: privatisation, militarisation and finally, their combination. Results included inconsistencies within the data of the necessary security incident records; inadequate competence and training among the PSO/PFSO; use of different procedures among the ports under investigation for dealing with exactly the same security issues; some port terminals were operating even though the PFSP and respective SOC had expired in 2014, two year prior this questionnaire being sent. It also found a significant improvement of inter institutional communication and coordination at the visited port where the “militarisation model” was being tested and where the port administration and Harbour Master positions were given to personnel from the Navy. It was concluded that after twelve years of the ISPS Code implementation, Mexico does not comply with the requirements of the ISPS Code at an acceptable level; and the lack of a national maritime security policy has resulted in a poor (maritime) security culture, despite the severe (security) challenges that this nation is facing. To see the detailed list of incidents found see the appended paper.
5.4 Paper 4: Mexico's reorganisation of maritime security regime: A new Role for the navy and emphasis on energy related infrastructures

Paper 4 presents a critical analysis of the latest maritime reform in which Mexico provides the legal framework to shift the National Maritime Authority from a civil institution (SCT) towards a military one (SEMAR). It also examines its extent of harmonisation with international law in respect of the ISPS Code implementation and compliance; and the level of acceptance of such changes, between the four pillars of representatives of authorities/institutions directly related to duties and operations, as Directors of Customs Maritime Units; Port Administrations Directors and PFSO; Commanders of the Navy and Harbour Masters.

The results of the critical analysis of the maritime reform, highlights several contradictions and ambiguities of the new regime, since several duties and responsibilities are still “shared”. While the SEMAR is responsible for implementation and compliance with the ISPS Code, the SCT is holding the port authority role and is responsible for imposition of sanctions related to violations of the Code. In addition, a significant inconsistency is that the decree modifies Article 7 of the “Law of Navigation and Maritime Trade” and establishes that the “National Maritime Authority” is exercised by the Federal Executive Power through SEMAR for the exercise of national sovereignty, deal with maritime safety and security issues, as well as exercise the Right of the State to be applied at the Mexican marine zones, while Article 9 B establishes that SCT will exercise its functions at the ports through the Offices of Services to the Merchant Marine. Additionally, the “Law of Ports”, Article 16, clearly established that the Port Authority is exercised by the Federal Executive Power through SCT, which in practice, would be exercised through the “Offices of Services to the Merchant Marine” established at all ports.

In 2014, the Mexican government attempted the reorganisation of its maritime security regime. Several existing laws were revised and a new set of regulations was introduced including amendments to the “Law of Ports” and the regulation in relation to the establishment of the CUMAR, which is the organ responsible for the implementation and compliance of the ISPS Code in this nation. However, since this attempt, the Parliament has focused on port security and port installations. They overlooked including in the regulation the part related to maritime security and the requirements for ships, established in the ISPS Code, such as the Ship Security Officer (SSO), Ship Security Assessment (SSA), the Ship Security Plan (SSP) and the International Ship Security Certificate (ISSC). This part was not revised either in the major maritime reform of 2017. From April 21st 2014 to June 2017, when the last updates to this chapter were made, there was no institution appointed as
responsible for maritime security in respect of vessels conforming Mexico’s national legislation.

It was established in Article 19 TER, paragraph II, of the Law of Ports, since the maritime security reform that took effect on the 21st of April 2014, that “the CUMAR shall apply all the dispositions and response measures within the framework of the Chapter XI-2 of the SOLAS 1974 Convention, comprising the ISPS Code and ensure the establishment of a series of functions and actions for each of the respective three security levels”. But, because of poor knowledge about the reform itself, the SEMAR did not exercise its authority and SCT through FIDENA directly revised and approved the PSA/PFSA and respective PSP/PFSP for the consequent issuance of SOCs, without taking into consideration the legal procedures regarding the CUMAR. After the last reform of 2016 the CUMAR kept this responsibility as established in Article 19 TER, of the Law of Ports, where there are clear specifications for each of the three maritime security levels.

PSP/PFSP and SSP were not revised and approved by the organ responsible for such action. Thus, SOCs and ISSC were not issued in accordance to the juridical procedures and must be revised and renewed, following the procedures established by law. The paper also highlights the unnecessary “inter institutional character” of the “CUMAR”, once the control and management of Harbours Masters was transferred to SEMAR.

Concerning the level of acceptance of this reform between those involved in port and maritime operations; the results show that from the interviewed subjects with functions of Harbour Masters, 75% expressed their approval of being transferred to the SEMAR and supported the law decree, while 25% strongly disapproved the transferral between the institutions. An important conclusion is that people interviewed were either very much in favour or very much against the change. 87.5% of Directors of Customs Maritime Units and 75% of Directors of FIPAs supported the law decree; at the same time, 100% of Presidents of CUMAR held a positive view. Same figures correspond to Commandants from the UNAPROP (coast guard-navy unit), whereas 87.5% from PSO supported the transferral of Harbour Masters to SEMAR; and 80% from interviewed subjects functioning as PFSO from hydrocarbon terminals supported the transfer.

As presented in Paper 4, twelve categories were identified that either prevent or promote the transferral of Harbour Masters from SCT to SEMAR:

I) Poor performance of Harbour Masters from the SCT;
II) Acute lack of human and material resources available for Harbour Masters to comply with their duties and responsibilities in a satisfactory manner;
III) High exposure to corruption on the part of Harbour Masters related to Mexican criminal organisations due to death threats against them or their families;

IV) Fear losing their jobs on the part of Harbour Masters in a later stage of their productive life;

V) Uncertainty on the part of Harbour Masters with respect to their salary levels, working rights and pension schemes;

VI) Improvement of salary and working rights for Harbour Masters and their personnel with the transferral to SEMAR;

VII) Already high participation of the Mexican Navy performing duties that correspond to Harbour Masters;

VIII) Fear on the part of Directors of Port Administrations concerning lack of knowledge, stubbornness and unwillingness/inflexibility to negotiate on factors related to business issues with respect to authorities from the Mexican Navy;

IX) (Trust in) Security improvement for offshore installations and vessels serving the oil market;

X) Trust in a significant improvement of maritime safety and security on the part of Directors of Customs Maritime Units with the transferral of Harbour Master offices to the SEMAR;

XI) Bigger and better capabilities (from SEMAR) to combat criminal organisations that are using port installations for the transport of drugs, weapons, money laundering and transport of stolen hydrocarbons, and finally;

XII) Need of providing juridical support and attributions to the SEMAR to activities already performed by the Navy and which currently are outside their juridical attributions.

5.5 Paper 5: Integrating the procedures of reporting port security incidents and the follow-up investigation to build a national maritime security policy: A case study in Mexico

Paper 5 presents the findings of the study about the implementation and compliance of the ISPS Code in respect of report and investigation of port security incidents and the results of an action research study, where an analytical transparent incident-
reporting tool developed by the researchers was implemented at all ports in Mexico where the ISPS Code applies, with the support of the National Maritime Authority. The aim is improving reporting of security incidents, allowing major insight in the problem areas to be integrated into PFSA, facilitating amendments to PFSP and enabling port/maritime security incident investigation. It is argued that by acquiring all relevant information of a particular event in this security incident-reporting tool; it would facilitate in learning from that particular security incident and use it not only for updating PSA/PFSA and respective PSP/PFSP, but also, to provide official security incidents investigators with all the necessary information, to investigate the event and instruct the implementation of measures that could prevent the re-occurrence of such event. It is suggested that the use of this tool combined with statistics provides the fundament for a multilevel analysis of port security threats, identifying the problem areas and contributing to set up the strategies for the development of a national maritime security policy.

On the basis of the interviews and observations to evaluate the implementation and compliance of the ISPS Code, in respect of report and investigation of port security incidents, fifteen themes were identified across the studied groups [CUMARs & UNAPROPs; Port Administration Directors; Customs Maritime Unit Directors; PSO/PFSO and Harbour Masters]; that affect port security either in a negative or positive way.

It is important to emphasise that these findings were made on the basis of the visits to ports and interviews before the transferal of the National Maritime Authority from the SCT to SEMAR, which entered into force on 17th of June 2017. However, the CUMAR was responsible for implementation and compliance of the ISPS Code since 21st April, 2014. The themes (which are presented in paper 5), are the following:

I) High discontent among Customs Maritime Units Directors concerning the rotation of customs authority agents between Customs Maritime Units, Airport Units and Cross-Border Units;

II) High reluctance by Port Administration Directors and PSO to allow port security authorities from the CUMAR and the UNAPROP permanent interconnection to CCTV systems in real time;

III) High reluctance by port terminals managers and PFSO to allow PSO and the UNAPROP permanent interconnection to CCTV systems in real time from port facilities (terminals) installations;

IV) High reluctance by Customs Maritime Units Directors to allow port security authorities from the CUMAR and the UNAPROP permanent interconnection to CCTV systems in real time concerning customs warehouse and other vulnerable customs areas;
V) Separate IT and CCTV systems rooms between naval authorities and customs authorities;

VI) High reluctance by port terminals managers and PFSO to share their PFSP with the representatives from port security authorities from the CUMAR (responsible for inspection and approval of PFSP) in order to inspect it, revise it and approve it and to develop the PSP for MARSEC (maritime security) level 3, responsibility of the CUMAR;

VII) Poor development of maritime security exercises at level 3, most performed without access to PFSP from port (terminals) facilities [exercises to be conducted once every calendar year, with no more than 18 months between them];

VIII) Lack of human and material resources at the UNAPROPs to cope with the ISPS Code duties;

IX) Poor development of PSP. Port Security Officers only consider risks and threats related to common port areas, installations and roadways within the port, but not for each of the port facilities (terminals) located within the port, neither analyse the impact of security incidents of the terminals against each other and particularly, specific high risks terminals against other considered of less risks.

X) Poor training of private security agents concerning port security risks and threats, as well as use of fire weapons.

XI) Satisfactory level of cooperation between the Customs Maritime Units authorities and the UNAPROPs for inspection of goods and vessels at the customs warehouse with ZVB and other no intrusive security systems. The ZVB is a mobile screening system using X-Ray for screening of cargo and vehicles. It uses a backscatter technology to provide photo-images of suspected objects within the cargo such as explosives, currency, drugs, psychotropic materials, forbidden chemicals, and trade-fraud items;

XII) With the exception of one port, none existence of official records of port and maritime security incidents (before the implementation of the “trans-parent incident reporting tool”);

XIII) None existence of PFSP’s amendments officially requested by port security authorities following port security incidents;

XIV) None existence of official reassessment of PSA/PFSA requested by port security authorities following port security incidents;
Concerning implementation and results of the “transparent incident reporting tool”, the results show a significant improvement in reporting port security incident records, which increased from zero to 57 during the first year of this tool implementation. During the first quarter 2017, twenty port security incidents were reported. For the second quarter, same year, the figure was nine, which represented a decrease of 55.00 per cent, compared to the first quarter. During the third quarter, a total of seventeen port security incidents were recorded, which represents an increase of 88.88 per cent, compared to the previous quarter. For the fourth quarter, eleven port security incidents were reported. This represents a decrease of 35.29 per cent, compared to the previous period. In addition, 56% of the reported maritime incidents followed recommendations to be integrated into the PFSA and to be considered for improvement of PFSP. However, none of such recommendations have been integrated into PFSA yet. The need for further training and competence about the ISPS Code, as identified in paper 3 is confirmed with the implementation of this tool. On three occasions members of the UNAPROP reported pure safety incidents as security incidents, which were not included in the macro analysis. The figures about reported security incidents per quarter, is presented in illustration 7.

Illustration 7 Graphic of port security incidents by quarter
As it can be observed in figure 8 below, the type of security incident that was reported most, is the code IFP-007, which stays for “confiscation of drugs, narcotics or psychotropic material”. The second place is shared by the classification codes IFP-006 (confiscation of weapons/firearms); IFP-009 (unauthorized access to restricted areas, including fishermen and stowaways); IFP-017 (vehicles abandoned in the port installations or its surroundings); IFP-019 (failures in control areas) and, the category “without code”. This type of incidents was assigned a code for the new quarter in relation to the period they were recorded.

![Illustration 8 Graphic of port security incidents by incident code](image)

In opposition to the significant improvement in respect of reporting security incidents, such progress was not reflected on consequent amendments to PSP/PFSP. However it does not necessarily mean that the recommendations for changes to PSA/PFSA and respective PSP/PFSP were ignored, but it must be taken into consideration that this type of process can take between six and twelve months; a period where they must be evaluated, tested, inspected and approved and they might be in a phase of this process. Anyhow the task has been problematic for members of the UNAPROP and representatives of the CUMAR since PSO/PFSO who have been very reluctant to deliver a copy of PSP/PFSP to the port security authorities from the CUMAR.

Other important findings are related to the location where the incidents took place. From a total of 57 port security incidents reported by the UNAPROP for the year 2017, 23 occurred within the Customs Maritime Unit Installations. As it is observed in figure 9 below, which represents a 40.35 per cent of the total of security incidents at port facilities.
From these 23 security incidents, four were about failure of access control to restricted areas and the precise discovery of unauthorized persons found within the customs restricted areas; and one more about discovery of suspicious packages within the customs area, all the rest involved confiscation of drugs, narcotics, psychotropic material and fire weapons in containers at the customs area. In one of the events, it was reported 800 units of grenades and pistols including AK-47 Rifles. The rest of security incidents at the customs installations involved confiscation of cocaine and chemical materials for the production of synthetic drugs illegally transported in containers by ships.

The findings related to serious deficiencies in the implementation and compliance of the ISPS Code in Mexico, within reporting of security incidents and its re-evaluation to PFSA and respective amendments to PFSP; the poor exercise of its authority from the CUMARs and UNAPROPs (SEMAR) in respect of fulfilling its obligations and responsibilities with respect to port and maritime security; and the remarkable improvement in reporting security incidents after the implementation of the “transparent security-incident-reporting tool”, which enables port/maritime security incident investigation and can serve to identify the problem areas; contributing to setting up strategies for the development of a national maritime security policy are some of the most relevant contributions of this dissertation.

Another important finding that should call for attention worldwide, is the fact that more than 40% of the reported security incidents occurred within the customs area, which even if it is within the port installations, is not required to conduct a security

Illustration 9 Port security incidents by quarter and port area
risk assessments and develop the respective security plan. It has already occurred in the past (as reported by one of the participants in the interview) that heavily armed members of criminal organizations have penetrated the port and customs installations to recover confiscated quantities of cocaine and materials for production of methamphetamines. This is evidence, that the lack of a risk assessment and security plan for installations of the Customs Maritime Units put at risk the whole port and its port facilities.
6. Discussion and conclusions

6.1 Evaluating the need of expansion to apply the ISPS Code to passenger ferries of less than 500 GRT and its respective port facilities

The annexed papers illustrate through different but connected topics, the rationing and purpose of the ISPS Code. They also highlight deficiencies and areas of opportunity for expansion of the application concerning this set of international security regulations to better secure oceans and port facilities.

Certainly the main focus of the ISPS Code is on terrorism. A number of theoretical scenarios about terror attacks have been tested around the globe and security measures have been thereby implemented. However, the Code does not apply to vessels of less of 500 GRT, including leisure craft. Medium and large ferries transporting travellers between tourist destinations in a specific State also fall out of this international security legislation.

Jones (2006) referred to a USCG study to point out that large ferries have been accounted with the highest risk assessment score from about 80 different maritime terrorist scenarios. The cited author writes:

“Ferries come in all shapes and sizes, and serve a multitude of different ports and trades. The largest ferries are indeed targets for terrorist, and they are extremely susceptible to devices brought on board by passengers”.

Because of the big number of people gathered in one specific place, public transport systems, including ferries, have been nominated as soft targets for terrorist organizations, appearing on the target list of different terrorist groups worldwide. Just a few months ago, on February 21st 2018, a terror attack against a large ferry with capacity for 300 passengers occurred in Mexico, when the craft arrived at the Cozumel port facility from Playa del Carmen, both close to Cancun, leaving 18 persons seriously injured (Sputnik, 2018), as previously discussed in section 2.2.3 of this dissertation. Different media sources published that a national drug crime organization announced the attribution of the event and the political motive behind, demanding the dismissal of the city mayor.
Lately, to cut construction cost of ferries, several yards have replaced steel with aluminium. Therefore concerns are growing about the ferry industry as well, as Jones (2006) wrote:

“The effect of a bomb of fire on such vessels can be catastrophic as aluminium is significantly weaker than steel when it undergoes heating and the effect of a terrorist attack could lead to the melting and destruction of an entire vessel extremely quickly. Aluminium melts at approximately 660 degrees C., whereas most commonly used steel melt at around 1370 degrees C, so the potential for an earlier degradation in the event of fire is obvious”.

One solution to this problem, would be to expand the application of the ISPS Code regarding the requirement of the SSA, PFSA, SSP and PFSP as well as the hire of SSO and PFSO to medium and large ferries and port facilities serving this type of naval craft and services. Additionally, construction rules for passenger ferries at the State level should be revised to limit the use of aluminium, reducing the risk level of a potential catastrophe.

Stricter security measures for the access of leisure craft and small fishery vessels, as well as high speed fibre boats used for fishery to port facilities should also be evaluated. During the participant observation phase of this study it was registered several small boats and high speed craft used for fishery within the navigation channels and in restricted seaways areas of the ports. It is important to recall that small boats are used for performing terror attacks against vessels and ports by deploying explosives, in most of the designed theoretical scenarios and tested worldwide in exercises for maritime security level 3, as the ISPS Code requires.

As expressed by (Dunham, 2004), the U.S.S. Cole (on 12 October 2000) and the French tanker Limburg (on 6 October 2002) were attacked by small vessels, whereas it was with small and high speed boats that al-Qaeda planned to blow up the Israeli Cruise ships off Turkey, as Jones (2006), pointed out.
In a hypothetical scenario that this boat had carried explosives and performed a terror attack, the consequences would have been catastrophic, since the tanker vessels could have exploded in chain and the explosions would have reached the oil tanks onshore, and in addition to loss of life and property, the marine environment devastation could have reached as far as coastal waters of the United States.

Stricter security measures are necessary to protect port facilities from small boats and leisure craft that might be used for terror attacks. The same risk factor also applies to marine oil platforms located in the Continental Shelf.

However, measures must include solutions for affected citizens at port cities, as in the case illustrated in the figure above, where locals use small boats to cross from one side to the other without subject to any control, crossing the main navigation channels, putting at high risks oil terminals.

6.2 The inherent role of the ISPS Code in keeping ports and vessels free of illegal traffic of drugs, weapons and unlawful items & the use of the developed transparent tool for reporting of security incidents and development of a national maritime security policy

Several of the annexed papers discuss findings related to port security incidents connected to smuggling of drugs, psychotropic material and weapons. Although the IMO has left Contracting Governments to determine the extent to which the ISPS Code and particularly the maritime security measures shall apply to armed robbery, drug smuggling, stowaways, illegal migration and the security of dangerous goods, if the security measures established by the Code are strictly implemented at ship and port facilities, they would be sufficient to keep them free of illegal traffic of drugs, weapons and illegal items, considering access controls, control of unauthorised persons and security of the port perimeter area and waterways.

If an illegal carriage of drugs, weapons or unlawful goods is found within a port facility, on the vessel or in a container, it implicitly means that there has already been a security breach of the measures established by the ISPS Code, either at that port, at one of the previous ports of departure reported by the vessel involved, or in less common cases, at the vessel itself during bunkering or catering stores operations, which in some illicit cases are performed outside the port facility and without the necessary authorities inspection. There are also registered cases in Mexico and several South American ports where swimmers and divers affix drugs packages to the bulbous bow of vessels.
In Cartagena Colombia, the Federal authorities arrested 14 persons involved in such operations for hiding the drug to be transported in the vessels hulls while they lay at the port for loading and unloading operations (RCN Noticias, 2015), similar, reports come from Puerto Bolivar, La Guajira, Colombia (Rodriguez, 2015), as well as the port of Santa Elena, in Ecuador, where the Navy found 5.53 tons of cocaine in an adapted compartment outside the hull of the vessel which were supposed to be transported to Europe (La Prensa, 2017). Additionally, the same practice regarding packages adhered to the bulbous bow of the vessel have been reported in Panamanian ports, where the Federal authorities found 213 packages containing cocaine in this way (El Nuevo Diario, 2017). The same situation has been reported at Quetzal Port, in Guatemala, where suitcases with 281 packages containing cocaine were discovered adhered to the bulbous bow of a vessel by the Navy Police of that State (El Periodico, 2017). Mexico is not exempted of this threat. On January 3rd this year (2018), the UNAPROP commissioned to Port of Lazaro Cardenas, in Mexico confiscated 300 kilos of cocaine that were also adhered to the bulbous bow of a vessel with Liberian Flag with the United States as destination (Casillas, 2018).

The problem has also reached Peru, where the reported confiscations of drugs are not limited to merchant vessels, but even ships belonging to the Peruvian Navy, where Canadian authorities confiscated 28 kilos of cocaine (El Tiempo, 1996).

Therefore, special measures must be implemented at ports and port facilities as well as with the vessels themselves regarding increased lighting around the hull and at docks and berths, giving special attention to small boats and high speed craft that could serve for hiding of swimmers/divers, sailing or waiting in the vicinity of ships. On the other hand, divers could also be used to affix bombs to vessel hulls for detonation at the next port of arrival, in another country. As Jones (2006) says:

“Security must therefore begin at the point of loading. Any container to be shipped through a port must be loaded in an approved secure facility. These facilities should be secured against unauthorized entry and the loading process monitored by camera. In high risks areas, cargo and vehicle scanners must be employed and the images stored so that they can be crosschecked with images taken by inspectors at a trans-shipment or arrival destination (...). It is vital to understand that all parties to the movement of cargo now have responsibilities and that if one sector does not apply itself rigorously to security then the entire effort can fail”.

One solution for this increasing problem is strengthening underwater surveillance with remotely operated underwater vehicles (ROVS) specially designed for harbour security, equipped with sonar, acoustic technologies and cameras as the UK’s Cerberus Yacht Sonar system, which is a diver detection system that provides 360-degree sub-surface security protection using the Ocean Marine Systems (OMS) for retracting through-hull instrument hoist. “The hoist enables active sonar to be
deployed with the vessel in motion, resulting in continuous monitoring of subsurface activity around a vessel” (Jeffrey, 2017).

On the other hand, the ISPS Code does not directly consider security measures for the aerial space of ports, including security threats that drones pose to the security of ports, port facilities and vessels. Lately the use of drones for smuggling of cocaine has increased. Ports and port facilities should consider this new technological threat. The use of drones deploying or intending to deploy explosives by terrorist organizations has been documented in previous events. The risk for a drone to deliver explosives, drugs, weapons and currency to port, port facilities and vessels needs to be included in the PSA/PFSA/SSA and respective PSP/PFSP/SSP. Though the ISPS Code establishes requirements for “preventing the introduction of unauthorised weapons, incendiary devices or explosive to ships” to vessels and port facilities, it does not directly address the security of the aerial space and the connected risk of drones.

The IMO reports that they work in close cooperation with the World Customs Organization on matters related to prevention and suppression of drug smuggling on ships engaged in international maritime traffic and relevant authorities from member States worldwide. The Revised Guidelines for the Prevention and Suppression of the Smuggling of Drugs, Psychotropic Substances and Precursor Chemicals on Ships engaged in International Maritime Traffic were adopted by IMO's Maritime Safety Committee (MSC) through resolution MSC.228(82), on 7 December 2006; and by Facilitation Committee (FAL) through resolution FAL.9(34), on 30 March 2007.

The Organization adds that the aim is to enhance maritime security worldwide, with particular focus on developing countries through capacity-building activities, “which are conducted at national and regional levels, by the IMO sub-Division for Maritime Security and Facilitation (MSF) that operates under the auspices of the Maritime Safety Division (MSD), which in turn functions under the purview of MSC” (International Maritime Organization, 2018).

Although, as the 228(82) Guidelines for the prevention of smuggling of drugs establishes, there are no shipping routes free of illegal traffic of drugs, psychotropic substances, precursor chemicals and weapons; countries located in the Latin-American region are overrepresented in production and confiscation of drugs and precursor chemicals for production of synthetic substances, according to the World Drug Report of 2017 (United Nations Office on Drugs and Crime, 2017). All Centre and South American nations, excluding Chile, are considered as developing countries (varying from lower to upper middle income countries) by the Organisation for Economic Cooperation and Development (OECD). Therefore, they should be prioritized for the IMO capacity-building programme on maritime security.
The findings of this research illustrate the significant number of port security incidents related to smuggling of drugs, precursor chemicals and weapons. This is highly relevant since confiscation of drugs; illicit substances and weapons were not considered as a port security incident at the different ports in Mexico before the implementation of the transparent reporting incident tool developed by the researcher. As documented in the appended papers 3 and 5 the selected ports reported that they have not registered a security incident since the ISPS Code implementation, back in 2004. Incidents records are the cornerstone for conducting PSA/PFSA and the respective development of PSP/PFSP.

The transparent incident reporting tool developed by the researcher serves not only for reporting of security incidents but also for security incident investigation and protection of evidence material, as it includes the type of incident, code, description of the incident and / or protection failure, time, date and maritime terminal (place) of the security incident, support evidence’s documents, daily event’s report, extract of binnacle, diagrams, pictures, videos, audio recordings: yes no personal information (involved persons), description of damages, authorities involved, description of authorities response to the incident, recommendations to modify the PSP/PFSP, if the incident should warrant official investigation, if there are arrested persons and it is transparent since it is signed by the PFSO, the Director of the Port, the Chief Commander of the UNAPROP and the Chairman (President) of the CUMAR.

Together with the use of statistics by incident code and port/port facility at national level, this instrument provides the State with crucial information at a macro level to set up strategies for developing a National Maritime Security Policy by identifying threats and applying a risk-based approach to port and maritime security management, allowing the state to allocate material, economic and human resources as required at each port.

Although this instrument was successfully implemented and tested at all ports where the ISPS Code applies in Mexico, with most type of port facilities, it can easily be adapted to other countries worldwide facing the same problems. It can also be modified to include other type of incidents not considered in the format by adding the type of security incident and allocating the respective incident code.

Edgerton (2013), cited by Kusi (2015), said that when security strategies and measures are appropriately designed, functions as enablers, facilitating cost-effective and reliable operations for all stakeholders.

Bateman (2005), studied capacity building in respect of maritime security for the region Asia-Pacific, he said that many countries belonging to this region lack the capacity to provide adequate maritime security at a national level, under their national jurisdiction and to implement international security standards as required.
by the ISPS Code. The author highlighted factors as lack of political and social will; lack of maritime security awareness; ineffective arrangements for maritime jurisdiction and enforcement, and differing interpretations of the Law of the Sea. He referred to the UN Conference on Environment and Development (UNCED, 1992) to define capacity building in the terms of maritime security:

“Capacity-building encompasses the country's human, scientific, technological, organisational, institutional and resource capabilities. A fundamental goal of capacity-building is to enhance the ability to evaluate and address the crucial questions related to policy choices and modes of implementation among development options”.

Currently Mexico shows several of the weaknesses revealed by Bateman (2005), and generally the lack of political and social will, as well as lack of maritime security awareness among the authorities of SEMAR and SCT to politically cooperate for the development of a National Maritime Security Policy.

This also makes obvious the need for the development of a National Maritime Security Culture. The implementation of the “transparent incident reporting tool” can facilitate it by providing crucial information to set up the strategies related to policy choices.

6.3 The need for expansion of the ISPS Code to offshore facilities in Mexico

As discussed in section 2.3.2 of this dissertation, piratical acts against oil platforms and offshore facilities located in the Continental Shelf in the Gulf of Mexico have significantly increased during the last decade.

The list of security incidents, vary from armed robbery on oilrigs, robbery of valuable equipment on “abandoned platforms” (empty of crew on board, but still under production and connected to other facilities with high production levels), including lifeboats and heliports, cabling and pipes to wells. Until now there has been no reports on loss of life in direct connection to violence during these unlawful acts (at the sea). However, the improper and rash disconnection of pipes and cables to wells might causes explosions resulting with the loss of life of perpetrators and an extensive marine disaster.

Because of ambiguities to what constitutes piracy under international law, this criminal action cannot be counted as “piracy”. Under the UNCLOS definition, piracy events must occur in the high waters and outside the jurisdiction of any State, but it encompasses not only ships, but any “property” attacked by a ship for private
(economic) ends, whereas under the act established by the International Maritime Bureau, the location of the incident is irrelevant, as is the end (including terror and political motives), but it imposes the ship to ship rule, leaving oil rigs and offshore facilities outside this definition.

Mejía (2007) discusses the fact that while “the definition of piracy in international law is quite precise and detailed, it has not been updated to take into account the development of the modern regime of maritime zones”.

Although, in the hypothetical expansion of the term piracy under UNCLOS to include acts within territorial waters, it would only include the unlawful acts with violence or a threat of violence, leaving out robbery or plundering on board “abandoned” platforms, where the use of violence is unnecessary.

On the other hand it is important to highlight that until now, all robbed and plundered platforms, were owned by PEMEX, the Mexican State oil company and with Mexican registration number, and therefore both, the nationality and the territorial principles of law applies.

The relevant question would be about enforcement of jurisdiction, if oilrigs and oil marine platforms located in the Continental Shelf (of Mexico) in the Contiguous Zone or at the Exclusive Economic Zone (EEZ), with a foreign State flag suffer armed robbery on board or are plundered. In that case they could also make the claim under the jurisdiction of their Flag State. Mexico amended its Constitution and Energy Law to open the oil business market to private companies for the exploitation of oil reservoirs from deep waters with the approval and implementation of the Constitutional Energy Reform, which became effective on December 21st 2013. On August 12th 2014 the new Hydrocarbons Law and the new Hydrocarbons Revenues Law became effective. These are part of a set of new laws and legal amendments to the energy reform (Cross & Patten, 2014).

With the opening of the oil market, security threats against critical infrastructure as offshore installations may increase, including activities associated with terrorism, considering the establishment of oil companies that have already experienced terror acts in the past, such as the Norwegian Statoil.

The security situation described above concerning offshore facilities needs to be improved. Part of this solution could be to expand the application of the ISPS Code instruments, declaring oilrigs and offshore facilities as port facilities, extending the requirements for the appointment of a PFSO, the development of a PFSA and the respective implementation of PFSP. By considering armed robbery into their PFSA and PFSP, offshore facilities would be better prepared for that type of events, improving their response to these type of incidents.

As explained in paper 1 of this dissertation, in the hypothetical scenario of a large terrorist attack on oil terminals, or even a marine casualty as a result of a security
incident, it is necessary that the PFSP should include procedures and measures for response to this type of emergencies, including the environmental factor. An attack against this type of infrastructure would require extensive coordination not only at national level, but also international.

Therefore the development of a plan for bi-national coordination with the neighbouring State, United States, putting aside sovereignty concerns and focusing on cooperation to avoid and manage (in this case) an extensive marine catastrophe is recommended.

Another solution is as Menefee (2002), argues Governments worldwide could develop a law under their national legislation to sanction acts of piracy and maritime violence committed within territorial waters or at the coastal zone. In the model presented by this author offshore installations are also considered for sanctions of maritime violence.

6.4 The enactment of the ISPS Code into Mexico’s national legislation, the 2016 maritime reform and possible solutions to juridical ambiguities

The appended papers present several deficiencies concerning the implementation and compliance of the ISPS Code in Mexico. Errors in the enactment of the Code into national legislation are exacerbated by the lack of cooperation between SEMAR and SCT for the adequate operation of the CUMARs at all ports, which is the organ that holds the responsibility for the revision and approval of PSA/PFSA PSP/PFSP SSA and SSP, audits and annual inspection on compliance of security plans.

One of the most serious deficiencies is the fact that due to the rather weak exercise of authority on the part of the representatives of the Navy at the CUMARs at all ports, and ignorance about their duties and responsibilities according to the Law of Ports and the CUMAR’s Regulation; the juridical procedures for the the revision and approval of PSA/PFSA PSP/PFSP and the issuance of respective SOCs to ports and port terminals were not followed. The void left by the CUMARs was in practice filled by FIDENA (through an agreement with SCT), which performed the revision, approval and inspections of security assessments and plans and send the respective notification of approval to SCT for issuance of issuance of the Statement(s) of Compliance and International Ship Security Certificates. Hence the current security plans and respective SOCs at all ports in Mexico must be revised and renewed, since they were not originally approved by the CUMAR, but by another institution violating the requirements established in the Law of Ports, articles 19; 19 BIS, and
19 TER; as well as the CUMAR’s regulation, as explained in paper 4 and section 2.2.3 of this dissertation.

Because of ambiguities and contradictions in several laws, the CUMAR has not been fully operating, inclusive after the last reform. This situation must be seen in light of the rather limited work of the National Parliament in respect of the inadequate enactment of Chapter XI-2 of the Safety of Life at Sea Convention 1974, (SOLAS Convention), containing the ISPS Code into national legislation in Mexico. This, together with the poor cooperation between SEMAR and SCT has resulted in the fact that the juridical procedures for the revision and approval of all PSA(s), PFSA(s), PSP(s), PFSP(s), and SSA(s), SSP(s) and and the issuance of respective Statement of Compliance (SOC) and International Ship Security Certificate(s), were not followed even after the last reform. The problem was regarding the revision and approval of those security evaluations and plans by the CUMAR, which was done by another institution that has not that attribution by law.

The significant deficiencies of the new maritime regime, including the “inter institutional character” of the CUMAR [completely unnecessary after the transferal of Harbour Masters to SEMAR] are presented in paper 4 and section 2.2.3 of this dissertation.

The magnitude of juridical weaknesses of the national legal framework, even after the last maritime reform, limit the exercise of authority of the “National Maritime Authority”, the CUMARs and UNAPROPs before national vessels, its masters and ship-owners; port administrations and port terminals to an obvious and outstanding degree.

Port and maritime security in the terms of the ratified international treaties and instruments (ISPS Code), is established as one of several attributions of SEMAR, according to the Organic Law of the Federal Public Administration, Article 30, subsection V, letter d. On the contrary, Article 36, subsection XVII of the same law, does not allocate this attribution to SCT, instead it establishes that SCT shall “participate” with SEMAR in the application of maritime safety and security measures.

The endorsed duty to SCT is on a “participation” level and only regarding maritime and not port security, since this is not reflected in the article as it is in the case of SEMAR. It is important to highlight that the Organic Law of the Federal Public Administration is above the Law of Ports, since that law establishes the attributions of each of the different secretariats of the State. Thus, port and maritime security is a total responsibility of SEMAR and the “inter institutional character” of the CUMARs is unnecessary.

A reasonable solution is that the President disregards the “inter institutional character” of the CUMAR established in the Law of Ports by a decree and gives full
attributions to SEMAR concerning port and maritime safety and security, leaving to SCT the responsibility for development of ports from an economic perspective, as it was intended with the 2016 reform and in harmonization with the established in the Organic Law of the Federal Public Administration.

Article 24 of the last referred Federal Law gives the power to the President to determine the attributions of an institution/ministry when there is disagreement between two laws or between two institutions. This Article reads as follows:

“In extraordinary cases or when exists doubts about the attributions of any of the Secretariats of the State related to a specific matter, the President of the Republic will resolve to which Secretariat corresponds its execution, through the Secretaría de Goverrbración, SEGOB (Secretariat of Governance)”. Such solution must be published in the Official Diary of the Federation.

This decree could also include the part of the ISPS Code related to vessels as the SSA, SSP and the designation of SSO, which was not included in the CUMAR’s Regulation in the sections dealing with the ISPS Code. Otherwise a revision to the CUMAR’s regulation is necessary.

The implementation of a national program for recertification of compliance the ISPS Code instruments at Mexican ports and vessels flagging its Flag to which the Code applies to, would be necessary as soon as the character and constitution of the CUMAR is solved. This is crucial not only for the national interest of Mexico and port stakeholders since it might have international and economic consequences, but also for ship-owners and charterers.

As previously discussed, ships must declare in the Advance Notice of Arrival the last 10 ports/port facilities where it has conducted loading and unloading operations. A ship that declares to have been at a port without a valid PSP/PFSP might be denied entrance to other ports in another country.

Additionally, a ship that lays in a port that does not comply with the required international security standards might not be secure. If it is not secure, it might not be safe, either. There is an obligation for all ship-owners and charterers under marine insurance law, amongst others, to keep the vessel safe.

Ship-owners and charterers might be unprotected regarding marine insurance coverage for Hull Insurance, Protection and Indemnity Insurance (P&I Insurance) and Loss of Hire Insurance, in the case of a casualty or time lost if the ship is detained because of confiscation of drugs or weapons, while laying in port facilities that do not hold a valid SOC and which have not implemented an approved security plan.

Even the national interest of a State regarding protection of the marine environment might be vulnerable in the case of a marine disaster caused by a ship, to which
coverage for environmental liability under P&I insurance is denied, because of laying on a port without a revised and approved security plan and respective SOC by the correct institution and in accordance to procedures established by law.

Finally, the five questions that McTaggar (1998) considers regarding validity for an action research study has been clearly answered through this section, specifying the changes that were made through the implementation of the “transparent incident reporting tool” and highlighting the improvement in reporting of security incidents, as well as the legal changes concerning the latest maritime reform. It also emphasizes what was not changed pointing out the unnecessary inter-institutional character of the CUMAR.

It remarks that the allocation of the Port Authority to SSCT was confirmed in the analysis of the reform, as well as the poor level of compliance with the ISPS Code at the visited port facilities.

The fact that amendments to PSP and PFSP that should have been conducted after security incidents were ignored, was also highlighted, as well as the lack of enactment of the part of maritime security regarding the SSO, SSA and SSP into the CUMAR’s Regulation.

The fact that the proper operation of CUMARs at all ports is problematic because of its “inter-institutional character” as well as operational conflicts between SEMAR and SCT was properly documented.

### 6.5 Conclusions and recommendations

The transparent reporting-incident tool developed and tested through this study has been proven to be highly valuable for reporting of port and maritime security incidents, as discussed in Paper 5 and section 5.5 of this dissertation, where it is demonstrated a significant improvement in reporting security incidents, with the increase from absolutely nothing (zero) to 57 providing a strong indicator of success. Moreover, it joins three primary port/maritime security functions: a) reporting of port and maritime security incidents; b) classification and investigation of serious security incidents that require reassessments of the PSA/PFSA/SSA and amendments to the PSP/PFSP/SSP and finally; c) collection of evidence material related to the security incident.

This instrument, combined with statistics, also provides nations with crucial information about threats and needs for the allocation of economic, material and human resources, absolutely necessary to set up the strategies for the development of a Maritime National Security Policy. Its flexibility and adaptability makes possible its implementation at any State of the world. Therefore it could be
considered as an important contribution to the maritime realm for improvement of maritime security.

Additionally, a critical analysis of the implementation and compliance of the ISPS Code in Mexico, with special focus on port security both from a juridical and practical perspective, was conducted in this dissertation. The appended papers and different sections of this study illustrate the chaotic situation concerning port security, which prevail in the referred country. It clearly identifies several breaches concerning the compliance with this international set of security regulations, as well as potential risks, and security threats for port administrators, terminal operators, oil platforms, ship-owners, charterers and neighbouring countries. However, it also provides possible and practical solutions, identifying the necessary amendments and decrees to harmonise the national legal framework with international legislation as the revocation of the “inter institutional character of the CUMAR”, which is urgent to allow this organ operate and ensure compliance of the ISPS Code at all ports. Likewise it suggests investments to upgrade physical security at port facilities as the recommended acquisition of Cerberus Yacht Sonar systems for underwater surveillance to cope with threats connected to smuggling of drugs and psychotropic substances.

The described situation is quite serious, but it is already under improvement. The SEMAR has taken several actions to upgrade port and maritime security under the opportunities given by the limited maritime regime that currently applies, whereas SCT has taken several actions to improve physical security of port facilities. The problem remains concerning the procedures followed for the approval of PSA/PFSA/SSA, PSP/PFSP/SSP, annual inspections, audits and respective certificates, since this was not made in accordance with the requirements established by law. Another issue is the limited cooperation between these institutions. Therefore, it is necessary the implementation of an intensive programme for revision and approval of PSA/PFSA/SSA, and PSP/PFSP/SSP with respective issuance of Statements of Compliance and International Ship Security Certificates, after the inter-institutional character of this organ is solved and according to the procedures established by law. Strengthening of cooperation between SEMAR and SCT is a prerequisite for success.

The findings of this dissertation are highly valuable for the required amendments to the maritime regime in Mexico, whilst the instrument for reporting of security incidents and its related applicability for the development of a National Maritime Security Policy represents an important contribution not only for Mexico, but worldwide.
6.7 Further research

a) The expansion of the application of the ISPS Code to oil platforms and offshore activities. It has been described in this dissertation how oilrigs and offshore facilities are also highly exposed to piratical acts and terrorism. The evaluation of the application of the ISPS Code instruments as PFSA and PFSP need to be further explored under a holistic approach where interest of the oil industry are represented in the balance between security and economic aspects.

b) The expansion of the application of the ISPS Code’s instruments to Customs Maritime Units. Findings in Paper 5 of this dissertation show that maritime customs installations are highly exposed to security threats. The lack of a security plan at these units might also put in risk the rest of the port area. The application of the PFSA and PFSP to Customs Maritime Units could be explored to standardize all facilities within the port area and synchronize port authority security efforts.

c) The definition of piracy concerning both the location of the incident and the type of property, including oilrigs and platforms needs to be further evaluated.

d) Specific strategies applicable worldwide for the development of a National Maritime Security Policy should be explored. It is true that the different parts of the world regions have different security risks, but there are some common factors that could be considered while building policies.

e) Security Culture. The approach to security culture is different depending of the world region. Lessons from countries with a strong security culture could be evaluated for its adaptability to other regions through capacity building.

f) The transparent reporting-incident tool developed and tested through action research in this study could also be combined with the revised harmonized reporting procedures for reports required under SOLAS regulation I/21 and MARPOL, Articles 8 and 12, established in the MSC-MEPC.3/Circ.3. Another possibility is that the data acquired through this instrument could serve to revise and complement information obtained through MSC-
MEPC.3/Circ.3 and its respective format concerning the part addressing information from casualties involving dangerous goods or marine pollutants in packaged form on board ships and in port areas. It is important to recall that while MEPC.3/Circ.3 focuses on very serious and serious marine casualties and incidents, from the accidental or human factor perspective (safety), the instrument developed in this study addresses incidents from a strict security perspective. In other words, those intentionally caused by any person with the aim of damaging the vessel, port facility or marine environment, as well as threats related to armed robbery, drug smuggling, stowaways and illegal migration.
References


Instituto Nacional de Acceso a la Información. (2015). *SISI 1857200171515 (Answer to information requestment).*

Instituto Nacional de Acceso a la Información. (2015). *SISI 1857200255715 (Answer to information requestment).*


120


Appendix

APPENDIX I Format for reporting security incidents, English Version

APPENDIX II Format for reporting security incidents, (Formato de Incidentes de Protección), Spanish Version


APPENDIX IV Paper 2: Opening of offshore oil business in Mexico and associated framework to cope with potential maritime security threats.

APPENDIX V Paper 3: Enhancing Maritime Security in Mexico: Privatization, Militarization, or a combination of both?

APPENDIX VI Paper 4: Mexico's Reorganisation of Maritime security regime: A new role for the navy and emphasis on energy related infrastructures

APPENDIX I

Format for reporting security incidents,
English version.

Avila-Zuñiga-Nordfjeld, Adriana
Dalaklis, Dimitrios
<table>
<thead>
<tr>
<th>TYPE OF SECURITY INCIDENT</th>
<th>ASIGNED CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTACK TO THE PORT / PORT INSTALLATIONS</td>
<td>IFP-001</td>
</tr>
<tr>
<td>BOMB OR EXPLOSIVES WARNING / TERRORISM</td>
<td>IFP-002</td>
</tr>
<tr>
<td>PERSONNEL KIDNAPPING WITHIN THE PORT INSTALLATION</td>
<td>IFP-003</td>
</tr>
<tr>
<td>PERSONNEL KIDNAPPING OUTSIDE THE PORT INSTALLATION</td>
<td>IFP-004</td>
</tr>
<tr>
<td>ARMED ROBBERY</td>
<td>IFP-005</td>
</tr>
<tr>
<td>CONFISCATION OF WEAPONS/FIREARMS</td>
<td>IFP-006</td>
</tr>
<tr>
<td>CONFISCATION OF DRUGS, NARCOTICS OR PSYCHOTROPIC MATERIAL</td>
<td>IFP-007</td>
</tr>
<tr>
<td>CONFISCATION OF EXPLOSIVES</td>
<td>IFP-008</td>
</tr>
<tr>
<td>UNAUTHORIZED ACCESS TO RESTRICTED AREAS (INCLUDING FISHERMEN AND STOWAWAYS)</td>
<td>IFP-009</td>
</tr>
<tr>
<td>UNAUTHORIZED ACCESS TO PORT AUTHORITY AREA (CUSTOMS / PORT POLICE)</td>
<td>IFP-010</td>
</tr>
<tr>
<td>UNAUTHORIZED DISCLOSURE OF PSP/PFSP’S INFORMATION</td>
<td>IFP-011</td>
</tr>
<tr>
<td>LEARNING TO KNOW SECURITY INCIDENTS BY THE MEDIA (NOT REGISTERED BEFORE)</td>
<td>IFP-012</td>
</tr>
<tr>
<td>TROUBLE/DAMAGE IN CCTV SYSTEMS</td>
<td>IFP-013</td>
</tr>
<tr>
<td>DAMAGE TO EQUIPMENT AND PROTECTIVE MEANS THROUGH VANDALISM</td>
<td>IFP-014</td>
</tr>
<tr>
<td>SUSPICIOUS PACKAGES IN THE PORT INSTALLATION OR THEIR SURROUNDINGS</td>
<td>IFP-015</td>
</tr>
<tr>
<td>ACCESS POINTS PROVIDED WITH INADEQUATED PROTECTION MEANS</td>
<td>IFP-016</td>
</tr>
<tr>
<td>VEHICLES ABANDONED IN THE PORT INSTALLATIONS OR ITS SURROUNDINGS</td>
<td>IFP-017</td>
</tr>
<tr>
<td>INAPPROPRIATE USE OF ACCESS DOCUMENTS FOR VISITORS</td>
<td>IFP-018</td>
</tr>
<tr>
<td>FAILURES IN CONTROL AREAS</td>
<td>IFP-019</td>
</tr>
<tr>
<td>EXTORTION'S TELEPHONE CALLS</td>
<td>IFP-020</td>
</tr>
<tr>
<td>WORKER'S STRIKE OR DEMONSTRATION WITH CLOSURE OF ACCESS AREAS</td>
<td>IFP-021</td>
</tr>
<tr>
<td>FAILURE IN THE TELEPHONE SYSTEMS</td>
<td>IFP-022</td>
</tr>
<tr>
<td>FAILURE IN THE WATER, ELECTRICITY OR SEWAGE SYSTEMS</td>
<td>IFP-023</td>
</tr>
<tr>
<td>UNAUTHORIZED DISSEMINATION OF CONFIDENTIAL MATERIAL</td>
<td>IFP-024</td>
</tr>
<tr>
<td>UNAUTHORIZED DISSEMINATION OF INFORMATION ON COMMERCIAL PROPERTY</td>
<td>IFP-025</td>
</tr>
<tr>
<td>UNAUTHORIZED DISSEMINATION OF INFORMATION WHICH MAY DAMAGE PORT SECURITY</td>
<td>IFP-026</td>
</tr>
<tr>
<td>INADEQUATED USE OF ACCESS DOCUMENTS AS ACCESS CARDS</td>
<td>IFP-027</td>
</tr>
<tr>
<td>STOWAWAYS</td>
<td>IFP-028</td>
</tr>
<tr>
<td>LOCALIZATION OF ILLEGAL IMMIGRANTS WITHIN THE PORT INSTALLATIONS</td>
<td>IFP-029</td>
</tr>
<tr>
<td>FAILURE TO PROTECT/HANDLE DANGEROUS GOODS</td>
<td>IFP-030</td>
</tr>
<tr>
<td>FAILURE TO USE ADEQUATE CLOTHING &amp; ACCESS IDENTITY CARDS WITHIN THE PORT INSTALLATIONS</td>
<td>IFP-031</td>
</tr>
<tr>
<td>FAILURE ON THE STRUCTURAL INTEGRITY OF THE PORT INSTALLATION</td>
<td>IFP-032</td>
</tr>
<tr>
<td>INAPPROPRIATE USE OF PERSONNEL EQUIPMENT MEANT PROTECTION SYSTEMS</td>
<td>IFP-033</td>
</tr>
<tr>
<td>FAILURE TO FOLLOW REGULATIONS AND PROCEDURES OF THE PORT INSTALLATION MEANT FOR PROTECTION</td>
<td>IFP-034</td>
</tr>
<tr>
<td>FAILURE ON RADIO AND TELECOMMUNICATION SYSTEMS</td>
<td>IFP-035</td>
</tr>
<tr>
<td>FAILURE IN COMPUTER SYSTEMS AND INFORMATIC NETWORKS</td>
<td>IFP-036</td>
</tr>
<tr>
<td>DETECTION OF ZONES THAT SERVE AS POINTS OF OBSERVATION FOR ILLICIT PURPOSES</td>
<td>IFP-037</td>
</tr>
<tr>
<td>RECOGNITION, WITHOUT DISCRIMINATORY CHARACTER, OF PERSONS WITH CHARACTERISTICS OR BEHAVIORAL PATTERNS THAT SUPPOSE A THREAT</td>
<td>IFP-038</td>
</tr>
<tr>
<td>NOT AUTHORIZED COMMERCIAL PRACTICES IN THE INTERFACE SHIP - PORT TERMINAL</td>
<td>IFP-039</td>
</tr>
<tr>
<td>LATE RESPONSES TO AN EMERGENCY OR CONTINGENCY PLANS</td>
<td>IFP-040</td>
</tr>
<tr>
<td>SECURITY INCIDENTS IN LOAD SPACES/WAREHOUSES AND STOWAGE DEVICES</td>
<td>IFP-041</td>
</tr>
<tr>
<td>DETECTION OF FAILURES IN THE EMERGENCY OR RESERVE EQUIPMENT AVAILABLE</td>
<td>IFP-042</td>
</tr>
<tr>
<td>INADEQUATED HANDLING OF THE CARRIAGE OR ESSENTIAL EQUIPMENT OF SYSTEMS OF THE PORT INSTALLATION</td>
<td>IFP-043</td>
</tr>
<tr>
<td>FAILURE OF LOGISTICS OR DELIVERY AND RECEPTION OF PROTECTION EQUIPMENT/PROVISIONS TO THE PORT INSTALLATION</td>
<td>IFP-044</td>
</tr>
<tr>
<td>NON-AUTHORIZED INTRUSION TO EXTRICT RESTRICTED AREAS OF THE PORT INSTALLATIONS</td>
<td>IFP-045</td>
</tr>
<tr>
<td></td>
<td>NAME OF INCIDENT AND / OR PROTECTION FAILURE:</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>ASSIGNED CODE:</td>
</tr>
<tr>
<td></td>
<td>DESCRIPTION OF THE INCIDENT AND / OR PROTECTION FAILURE:</td>
</tr>
<tr>
<td></td>
<td>TIME, DATE AND MARITIME TERMINAL (PLACE) OF THE SECURITY INCIDENT OR PROTECTION FAILURE:</td>
</tr>
<tr>
<td></td>
<td>SUPPORT EVIDENCE'S DOCUMENTS:</td>
</tr>
<tr>
<td></td>
<td>DAILY EVENT'S REPORT:</td>
</tr>
<tr>
<td></td>
<td>EXTRACT OF BINNACLE:</td>
</tr>
<tr>
<td></td>
<td>DIAGRAMS:</td>
</tr>
<tr>
<td></td>
<td>PICTURES:</td>
</tr>
<tr>
<td></td>
<td>VIDEOS:</td>
</tr>
<tr>
<td></td>
<td>AUDIO RECORDINGS:</td>
</tr>
<tr>
<td></td>
<td>PERSONAL INFORMATION (INVOLVED PERSONS):</td>
</tr>
<tr>
<td></td>
<td>DESCRIPTION OF DAMAGES:</td>
</tr>
<tr>
<td></td>
<td>NOTIFICATIONS:</td>
</tr>
<tr>
<td></td>
<td>PSO / PFSO:</td>
</tr>
<tr>
<td></td>
<td>NAVY UNIT FRO PORT PROTECTION (NAUPRO) NR.:</td>
</tr>
<tr>
<td></td>
<td>MASTER OF HARBOUR:</td>
</tr>
<tr>
<td></td>
<td>ANY OTHER INSTITUTION:</td>
</tr>
<tr>
<td></td>
<td>NAME OF THE INSTITUTION:</td>
</tr>
<tr>
<td></td>
<td>EXACT PLACE WHERE THE SECURITY INCIDENT OR PROTECTION FAILURE HAPPENED:</td>
</tr>
<tr>
<td>#</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>-------------</td>
</tr>
<tr>
<td>8</td>
<td>DESCRIPTION OF AUTHORITIES RESPONSE TO THE SECURITY INCIDENT OR PROTECTION FAILURE:</td>
</tr>
<tr>
<td>9</td>
<td>TYPE OF INCIDENT OR PROTECTION FAILURE IF NOT INCLUDED IN THE CODE’S LIST:</td>
</tr>
<tr>
<td>10</td>
<td>CROQUIS/ SKETCH OF THE SECURITY INCIDENT PLACE:</td>
</tr>
<tr>
<td>11</td>
<td>PORT SECURITY PLAN / PORT FACILITY SECURITY PLAN:</td>
</tr>
</tbody>
</table>

**DID THE PSP/PFSP FUNCTION PROPERLY?**

- Yes
- No

**ARE THERE RECOMMENDATIONS TO MODIFY THE PSP/PFSP?**

- Yes
- No

**SPECIFY WHAT MODIFICATIONS ARE SUGGESTED TO DO:**
<table>
<thead>
<tr>
<th></th>
<th>COMMENTS AND RECOMMENDATIONS FROM THE PSO / PFSO:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WAY OF PARTICIPATION OF AUTHORITIES AND INSTITUTIONS:</td>
</tr>
<tr>
<td></td>
<td>SHALL THE SECURITY INCIDENT PASSES TO OFFICIAL INVESTIGATION OR BE FOLLOWED UP?</td>
</tr>
<tr>
<td></td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>WHICH AUTHORITY SHALL BE IN CHARGE OF THE OFFICIAL INVESTIGATION, IF NECESSARY?</td>
</tr>
<tr>
<td></td>
<td>WHICH OTHER AUTHORITIES INTERVENED IN THE OFFICIAL INVESTIGATION?</td>
</tr>
</tbody>
</table>
### Arrested Persons as a Result of a Security Incident:

**Are there arrested persons as a result of the security incident?**
- Yes
- No

**Names, last names, gender, age and other personal information of arrested persons:**

**Have they been involved in previous official investigations?**
- Yes
- No

**Authority, official investigation number, address of the authority/court and other related data:**

### General Comments:

ELABORATED BY
- PSO/PFSO

REVISED BY
- General Director of Port or Port Facility

Witness of the Elaboration
- UNAPROP Commander

V/O
- B/O
- CUMAR / Chairman of the Group

**Date**

**Revision**

**Book & File NR:**
APPENDIX II

Format for reporting security incidents,
Spanish version.

Avila-Zuñiga-Nordfjeld, Adriana
Dalakis, Dimitrios
<table>
<thead>
<tr>
<th>TIPO DE INCIDENTE Y/O FALLO DE PROTECCIÓN</th>
<th>CÓDIGO ASIGNADO</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATAQUE A LA INSTALACIÓN PORTUARIA</td>
<td>IFP-001</td>
</tr>
<tr>
<td>AVISO DE BOMBA O EXPLOSIVO</td>
<td>IFP-002</td>
</tr>
<tr>
<td>SECUESTRO DENTRO DE LA INSTALACIÓN PORTUARIA</td>
<td>IFP-003</td>
</tr>
<tr>
<td>SECUESTRO FUERA DE LA INSTALACIÓN PORTUARIA</td>
<td>IFP-004</td>
</tr>
<tr>
<td>ROBO A MANO ARMADA</td>
<td>IFP-005</td>
</tr>
<tr>
<td>LOCALIZACIÓN DE ARMA O ARMAS DE FUEGO</td>
<td>IFP-006</td>
</tr>
<tr>
<td>LOCALIZACIÓN DE ESTUPEFACIENTES O PSICOTROPICOS</td>
<td>IFP-007</td>
</tr>
<tr>
<td>LOCALIZACIÓN DE EXPLOSIVOS</td>
<td>IFP-008</td>
</tr>
<tr>
<td>ACCESO NO AUTORIZADO A UNA ZONA RESTRINGIDA (INCLUYENDO PESCADORES Y POLIZONES)</td>
<td>IFP-009</td>
</tr>
<tr>
<td>ACCESO NO AUTORIZADO A LA AUTORIDAD PORTUARIA</td>
<td>IFP-010</td>
</tr>
<tr>
<td>DIVULGACION NO AUTORIZADA DE UN PPIP</td>
<td>IFP-011</td>
</tr>
<tr>
<td>CONOCIMIENTO DE UN SUceso POR LOS MEDIOS DE COMUNICACION</td>
<td>IFP-012</td>
</tr>
<tr>
<td>FALLO EN LOS SISTEMAS DE CCTV</td>
<td>IFP-013</td>
</tr>
<tr>
<td>DANO A LOS EQUIPOS Y MEDIOS DE PROTECCION MEDIANTE VANDALISMO</td>
<td>IFP-014</td>
</tr>
<tr>
<td>PAQUETES SosPECHOSOS EN LA INSTALACIÓN PORTUARIA O SUS INMEDIACIONES</td>
<td>IFP-015</td>
</tr>
<tr>
<td>PUNTOS DE ACCESO PROVISTOS DE INADECUADOS MEDIOS DE PROTECCIÓN.</td>
<td>IFP-016</td>
</tr>
<tr>
<td>VEHICULOS ABANDONADOS EN LA INSTALACIÓN PORTUARIA O SUS INMEDIACIONES</td>
<td>IFP-017</td>
</tr>
<tr>
<td>USO INADECUADO DE PASES</td>
<td>IFP-018</td>
</tr>
<tr>
<td>FALLOS EN LOS PUNTOS DE CONTROL</td>
<td>IFP-019</td>
</tr>
<tr>
<td>LLAMADA TELEFÓNICA DE EXTORSIÓN</td>
<td>IFP-020</td>
</tr>
<tr>
<td>HUELGA O MANIFESTACIÓN DE TRABAJADORES CON CIERRE DE ACCESOS.</td>
<td>IFP-021</td>
</tr>
<tr>
<td>FALLO EN LOS SISTEMAS DE TELEFONIA</td>
<td>IFP-022</td>
</tr>
<tr>
<td>FALLO EN LOS SERVICIOS DE AGUA, ELECTRICIDAD O DRENAJE.</td>
<td>IFP-023</td>
</tr>
<tr>
<td>DIFUSION NO AUTORIZADA DE MATERIAL CONFIDENCIAL</td>
<td>IFP-024</td>
</tr>
<tr>
<td>DIFUSION NO AUTORIZADA DE INFORMACION SOBRE PROPIEDAD COMERCIAL.</td>
<td>IFP-025</td>
</tr>
<tr>
<td>DIFUSION NO AUTORIZADA DE INFORMACION QUE PUEDA MENOSCABAR A LA PROTECCION.</td>
<td>IFP-026</td>
</tr>
<tr>
<td>USO INDEBIDO DE DOCUMENTOS DE ACCESO.</td>
<td>IFP-027</td>
</tr>
<tr>
<td>POLIZONES</td>
<td>IFP-028</td>
</tr>
<tr>
<td>MIGRACIÓN ILEGAL</td>
<td>IFP-029</td>
</tr>
<tr>
<td>FALLO EN LA PROTECCIÓN DE MERCANCIA PELIGROSA</td>
<td>IFP-030</td>
</tr>
<tr>
<td>FALLO EN EL USO DE VESTIMENTA ADECUADA DENTRO DE LA INSTALACIÓN PORTUARIA</td>
<td>IFP-031</td>
</tr>
<tr>
<td>FALLO EN LA INTEGRIDAD ESTRUCTURAL DE LA INSTALACIÓN PORTUARIA</td>
<td>IFP-032</td>
</tr>
<tr>
<td>USO INADECUADO DE EQUIPOS O SISTEMAS DE PROTECCION DEL PERSONAL</td>
<td>IFP-033</td>
</tr>
<tr>
<td>FALLO EN LAS NORMAS Y PROCEDIMIENTOS DE LA INSTALACIÓN PORTUARIA</td>
<td>IFP-034</td>
</tr>
<tr>
<td>FALLO EN LOS SISTEMAS RADIOELECTRICOS Y DE TELECOMUNICACIONES</td>
<td>IFP-035</td>
</tr>
<tr>
<td>FALLO EN LOS SISTEMAS Y REDES INFORMÁTICAS</td>
<td>IFP-036</td>
</tr>
<tr>
<td>DETECCION DE ZONAS QUE SIRVAN COMO PUNTOS DE OBSERVACION CON FINES ILCITOS</td>
<td>IFP-037</td>
</tr>
<tr>
<td>RECONOCIMIENTO, SIN CARÁCTER DISCRIMINATORIO, DE PERSONAS CON CARACTERÍSTICAS O PAUTAS DE COMPORTAMIENTO QUE SUPONGAN UNA AMENAZA.</td>
<td>IFP-038</td>
</tr>
<tr>
<td>PRACTICAS COMERCIALES NO AUTORIZADAS EN LA INTERFAZ BUQUE - PUERTO</td>
<td>IFP-039</td>
</tr>
<tr>
<td>RESPUESTA TARDIA ANTE UNA EMERGENCIA O PLANES PARA CONTINGENCIA</td>
<td>IFP-040</td>
</tr>
<tr>
<td>INCIDENTE EN LOS ESPACIOS DE CARGA Y DISPOSITIVOS DE ESTIBA</td>
<td>IFP-041</td>
</tr>
<tr>
<td>DETECCION DE FALLOS EN EL EQUIPO DE EMERGENCIA O DE RESERVA DISPONIBLE</td>
<td>IFP-042</td>
</tr>
<tr>
<td>MANIPULACION INDEBIDA DE LA CARGA, DEL EQUIPO O SISTEMAS ESenciaLES DE LA INSTALACIÓN PORTUARIA</td>
<td>IFP-043</td>
</tr>
<tr>
<td>FALLO EN LAS ENTREGAS Y RECEPCIONES LOGISTICAS DE PROVISIONES A LA INSTALACIÓN PORTUARIA</td>
<td>IFP-044</td>
</tr>
<tr>
<td>INTRUSION NO AUTORIZADA A AREAS RESTRINGIDAS DE LA INSTALACION PORTUARIA</td>
<td>IFP-045</td>
</tr>
</tbody>
</table>

**DOCUMENTO CONFIDENCIAL**
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NOMBRE DEL INCIDENTE Y/O FALLO EN LA PROTECCIÓN.</td>
<td>CÓDIGO ASIGNADO.</td>
</tr>
<tr>
<td>2</td>
<td>DESCRIPCIÓN DEL INCIDENTE Y/O FALLO EN LA PROTECCIÓN.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>HORA, FECHA Y TERMINAL MARÍTIMA (LUGAR) DEL INCIDENTE Y/O FALLO EN LA PROTECCIÓN.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>DOCUMENTACIÓN Y EVIDENCIA DE SOPORTE:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>REPORTE DE NOVEDADES:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>EXTRACTO DE BITÁCORA:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>DIAGRAMAS:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>FOTOGRAFÍAS:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>VIDEOS:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>GRABACIONES DE AUDIO:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>INFORMES PERSONALES:</td>
<td>SI</td>
</tr>
<tr>
<td>5</td>
<td>DESCRIPCIÓN DE DAÑOS:</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>NOTIFICACIONES:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPIP:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>UNAPROP-14:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>CAPITÁN DE PUERTO:</td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td>ALGUNA OTRA CORPORACIÓN:</td>
<td>SI</td>
</tr>
<tr>
<td>7</td>
<td>LUGAR EXACTO DEL INCIDENTE O FALLO EN LA PROTECCIÓN:</td>
<td></td>
</tr>
</tbody>
</table>

DOCUMENTO CONFIDENCIAL
PLAN DE PROTECCIÓN PORTUARIA / PLAN DE PROTECCIÓN DE LA INSTALACIÓN PORTUARIA
ADMINISTRACIÓN FEDERAL PORTUARIA INTEGRAL

NOMBRE DEL PUERTO: _______________________________________
INCIDENTE Y/O FALLO EN LA PROTECCIÓN: _______________________
NÚMERO DE FOLIO: _______________________________________

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8</strong></td>
<td><strong>DESCRIPTIÒN DE LA RESPUESTA AL INCIDENTE O FALLO EN LA PROTECCIÓN:</strong></td>
</tr>
<tr>
<td><strong>9</strong></td>
<td><strong>TIPO DE INCIDENTE Y/O FALLO EN LA PROTECCION:</strong></td>
</tr>
<tr>
<td><strong>10</strong></td>
<td><strong>CROQUIS DEL LUGAR DEL INCIDENTE:</strong></td>
</tr>
<tr>
<td><strong>11</strong></td>
<td><strong>PLAN DE PROTECCIÓN DE LA INSTALACIÓN PORTUARIA:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>SI</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FUNCIONÓ CORRECTAMENTE EL PPIP.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HAY RECOMENDACIONES PARA MODIFICAR EL PPIP.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ESPECIFICAR QUE MODIFICACIONES SE PROPONEN REALIZAR:**
PLAN DE PROTECCIÓN PORTUARIA / PLAN DE PROTECCIÓN DE LA INSTALACIÓN PORTUARIA
ADMINISTRACIÓN FEDERAL PORTUARIA INTEGRAL

NOMBRE DEL PUERTO: _____________________________________________
INCIDENTE Y/O FALLO EN LA PROTECCIÓN __________________________
NÚMERO DE FOLIO: _____________________________________________

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>COMENTARIOS Y RECOMENDACIONES DEL OPIP.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>PARTICIPACIÓN DE AUTORIDADES:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>EL INCIDENTE PASA A INVESTIGACIÓN OFICIAL O DE CONTINUIDAD:</td>
</tr>
<tr>
<td></td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>SI</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>¿QUE AUTORIDAD ES LA ENCARGADA DE LA INVESTIGACIÓN?</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>¿QUE OTRAS AUTORIDADES INTERVINIERON?</td>
</tr>
</tbody>
</table>

DOCUMENTO CONFIDENCIAL
NOMBRE DEL PUERTO: ____________________________
INCIDENTE Y/O FALLO EN LA PROTECCIÓN: ____________________________
NÚMERO DE FOLIO: ____________________________

<table>
<thead>
<tr>
<th>Fecha</th>
<th>Revisión</th>
<th>Libro y Foja</th>
</tr>
</thead>
</table>

¿HAY DETENIDOS?  ❒ SI  ❒ NO
NOMBRES, APELLIDOS, SEXO, EDAD Y OTROS GENERALES DE LOS DETENIDOS

¿HAY AVERIGUACIONES PREVIAS?  ❒ SI  ❒ NO
AUTORIDAD, NUMERO DE AVERIGUACIÓN, DOMICILIO DE LA AUTORIDAD Y OTROS DATOS.

COMENTARIOS GENERALES:

ELABORÓ
OPIP

REVISÓ
DIRECTOR GENERAL DE LA INSTALACIÓN

V/O  B/O
PRESIDENTE DE CUMAR

FECHA

LIBRO Y FOJA
Implementation and compliance of the International Ship and Port Facility Security Code in Mexico: A literature review and selected issues

Avila-Zuñiga-Nordfjeld, Adriana Dalaklis, Dimitrios


A. Ávila-Zúñiga-Nordfjeld & D. Dalaklis
World Maritime University, Malmö, Sweden

ABSTRACT: This paper provides a literature review of the state of the art on implementation and compliance of the International Ship and Port Facility Security Code (ISPS Code), for the case of Mexico. This investigation was initially oriented solely towards Mexico, but due to the absence of research within this subject for the referred country the review had to be done through subcategories with the conditional connection of Mexico and relevant issues were selected. The primary data confirmed the absence of research within this subject in Mexico. The secondary data, were other words related to the ISPS Code were used for the search, allowed for a wider geographical coverage and an expanded on general bases the scope of analysis, since ten (10) different academic databases were exploited. The literature review from an author-centric approach is initially presented; then, it is used as the basis to further develop (and examine) the concept-centric approach, through eight selected categories. The careful screening of literature, constructed on specific concepts, allowed the identification of cross fertilization of such concepts in the respective fields. It is observed that the research efforts focused on the ISPS Code and the development of a Port Facility Security Plan (PFSP) have an integrated perspective, where the categories of terrorism and counterterrorism, as well as maritime security management and the issue of port security have a strong interaction and dominant status. The results demonstrate the limited number of academic contributions in these areas from America Central and South America in relation to other parts of the globe, as well as the total absence of research efforts about the ISPS Code in Mexico. In the scientific contributions on the subject were Mexico is included; it is in reference to isolated cases of armed robbery, drugs organizations or proliferation of crime on general bases, but not regarding the ISPS Code itself. The absence of scientific research on this area for the specific country might also be related to the lack of a national maritime security policy and a poor maritime security culture as the authors have pointed out in other contributions.

1 INTRODUCTION

After the notorious terror attack in the United States of America (U.S.) on September 11th, 2001, the International Maritime Organization (IMO) developed a set of maritime security regulations for managing the risk of maritime terrorism with the aim to improve maritime and port security. These provisions were established in Chapter XI-2 of the Safety of Life at Sea Convention 1974, (SOLAS Convention), containing the new International Ship and Port Facility Security Code (ISPS Code). Part A of this Code establishes the mandatory provisions, while the non-mandatory (“recommended”) part B encompasses guidelines about how to comply with the mandatory requirements of part A (IMO, Official website, 2017).
The IMO establishes that the ISPS Code is “the comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States” (IMO, Official website, 2017). As explained by Nordfeld & Dalaklis (2016), compliance with the ISPS Code and submission of related information to IMO is only mandatory for Contracting Governments to the SOLAS 1974 Convention. They have also pointed out that currently “there is not a penalty-mechanism in place for states that don’t effectively comply with the ISPS Code”, since the overall concept is not to impose penalties, but to rely on market forces and economic factors to ensure compliance.

The development of Port Facility Security Plans (PFSPs) has been discussed within the context of maritime security management systems in several research efforts after the approval of the ISPS Code by the IMO; it has been viewed as the most important instrument to cope with potential security risks at ports and associated infrastructure-installations. Mexico implemented the ISPS Code in 2004 yet, the development/establishment of PFSPs has not been fully effective, especially regarding security incident reporting and investigation. Incident record keeping and the consequent investigation are crucial for the performance and applicability of PFSPs, since these Plans must be amended attending the causes of the investigated event.

As discussed by Webster & Watson (2002), an effective literature review is a crucial foundation for advancing knowledge, because it defines the key sources for a topic under research and uncovers the areas where (more) research is necessary, giving a clear contribution to science. Additionally, an effective literature review must follow academic guidelines to rigorously document the process of literature search as discussed by Brocke, et al. (2009); the literature review in hands strictly follows a linear and simple approach that ensures academic integrity. The foundation of the methodology used is presented in the next section; subsequently, the results are discussed, followed by the necessary conclusions.

2 OBJECTIVES

The objective of this paper is to examine the state of the art related to the implementation and compliance of the International Ship and Port Facility Security Code (ISPS Code) within the context of port security in Mexico, based on a cross-disciplinary approach among eight selected categories.

3 METHODOLOGY

Webster & Watson (2002, p. xiv) explained that a high quality review must cover all relevant literature on the topic and should not be confined to a limited set of journals. Therefore, a thorough search by topic in different databases across all relevant journals and across all disciplines must be performed. The contextual boundary is within the scope of the development of the PFSP for port oil terminals in Mexico, under the framework of the opening of the oil industry in that country; the respective time-based boundary covers all articles published in journals and conference proceedings until the indicated dates for search at the databases given in table 1 that follows. This table describes the considered databases for this literature review and the parameters for querying.

The literature search method encompassed querying ten (10) different scientific databases as proposed by Webster & Watson (2002, p. xvi). The first test was made back in June 2015, with the search queries for “ISPS Code Mexico”. This resulted in only one book review about military law. New tests with other words were tried. The key words used for the search criteria, excluding the Google Scholar Database, were “offshore, terrorism, Mexico”. Furthermore, since probably there are thousands of articles related to each of these concepts, testing different combination of them was required. Other combination of words were tested first, like “offshore, terrorism, resilience” and “offshore, terrorism, resilience, security management systems, ISPS Code”. It was discovered that these search enquiries covered a very few items. Additionally, the search “offshore, terrorism, ISPS Code, Mexico” was tried. At the end of the successive test queries, the keywords “offshore, terrorism, Mexico” was tested. This one provided the largest number of items; it was also noted that with this search query several articles included in the other tests were also included in the results (largest data sample). It is important to recall that the search for “ISPS Code Mexico” resulted in zero items and therefore, the words “offshore, terrorism, Mexico” were used with reasoning that ISPS Code focuses on terrorism and provides maritime security measures to counter terrorism both at ports and at sea and the condition that we were searching for results in Mexico. Other type of maritime security threats like piracy; armed robbery; stowaways; illegal migration; and drug smuggling, are not directly covered by the ISPS Code, since it leaves up to the discretion of contracting government to SOLAS, its extension of application to these type of subjects (IMO, 2012), and hence they were not considered for the search query.

Since the words used for querying the different databases were in English, the search included only academic journal articles written in English. However, for the Google Scholar Database another combination of words in Spanish was used; “Mexico, terrorismo, instalaciones portuarias petroleras, plan de protección”11. The time boundary was specified to 2004-2015 (after the ISPS Code was introduced). Even if the words were in Spanish, some articles in English were also captured by this search. It was decided to also use Google Scholar because several of the leading scientific journals in Spanish are indexed there. The considered databases for this literature review and the parameters for querying are all listed in Table 1.

11 Mexico, terrorism, oil port installations, security plan.
Table 1. Databases and parameters for search enquiry

<table>
<thead>
<tr>
<th>Database</th>
<th>Words of search</th>
<th>Date of search</th>
<th>Period &amp; Language of search</th>
<th>Nr. Articles</th>
<th>Relevant articles after title</th>
<th>Relevant articles after Abstract/Preface/Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) CRC-net-Base</td>
<td>Offshore terrorism</td>
<td>03.06.2015</td>
<td>Non specified</td>
<td>190</td>
<td>40</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Mexico (OTM)</td>
<td></td>
<td>(OTM)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) ProQuest</td>
<td></td>
<td>05.06.2015</td>
<td>Non specified</td>
<td>28</td>
<td>15</td>
<td>10&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>(3) Science-Direct</td>
<td></td>
<td>06.06.2015</td>
<td>Non specified</td>
<td>279</td>
<td>36</td>
<td>5</td>
</tr>
<tr>
<td>(4) Academic Search</td>
<td></td>
<td>06.06.2015</td>
<td>Non specified</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Complete WMU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5) Ingenta-Connect</td>
<td></td>
<td>06.06.2015</td>
<td>Non specified</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(6) Springer</td>
<td></td>
<td>06.06.2015</td>
<td>Non specified</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(7) Emerald Insight</td>
<td></td>
<td>21.08.2015</td>
<td>Non specified</td>
<td>82</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>Library</td>
<td></td>
<td>21.08.2015</td>
<td>Non specified</td>
<td>134</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td>(8) IEEExplore Digital</td>
<td></td>
<td>21.08.2015</td>
<td>Non specified</td>
<td>614</td>
<td>35</td>
<td>17</td>
</tr>
<tr>
<td>(OTM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(9) Wiley Online Library</td>
<td></td>
<td>22.08.2015</td>
<td>Non specified</td>
<td>614</td>
<td>35</td>
<td>17</td>
</tr>
<tr>
<td>(10) Google Scholar</td>
<td>Mexico terrorismo inst. Port.</td>
<td>2004-2015</td>
<td>22.08.2015</td>
<td>472</td>
<td>34</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>petroleras plan de seguridad&lt;sup&gt;1&lt;/sup&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td></td>
<td></td>
<td>1801</td>
<td>194</td>
<td>73</td>
</tr>
</tbody>
</table>

On 2<sup>nd</sup> of March, 2018 and with an effort to re-evaluate the state of the art and update the results, a new test with the search query “ISPS Code, Mexico” was conducted. This time it was made only in EBSCO since this scientific search instrument covers all the databases above, the results showed only one item. To ensure that it was the right search query and avoid human bias; the words “ISPS Code” but in combination with several other countries were further tested. These results are provided in Table 2.

Table 2. Number of research contributions by the combination of ISPS Code and the country

<table>
<thead>
<tr>
<th>ISPS CODE + COUNTRY</th>
<th>NR. OF CONTRIBUTIONS / ARTICLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>29,107</td>
</tr>
<tr>
<td>Europe</td>
<td>15,276</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>27,442</td>
</tr>
<tr>
<td>Greece</td>
<td>12,809</td>
</tr>
<tr>
<td>Turkey</td>
<td>12,721</td>
</tr>
<tr>
<td>Sweden</td>
<td>13,447</td>
</tr>
<tr>
<td>Norway</td>
<td>12,915</td>
</tr>
<tr>
<td>Canada</td>
<td>4</td>
</tr>
<tr>
<td>Mexico</td>
<td>1</td>
</tr>
<tr>
<td>Brazil</td>
<td>13,015</td>
</tr>
<tr>
<td>Argentina</td>
<td>12,641</td>
</tr>
<tr>
<td>Chile</td>
<td>12,645</td>
</tr>
<tr>
<td>Peru</td>
<td>12,529</td>
</tr>
<tr>
<td>Panama</td>
<td>12,648</td>
</tr>
</tbody>
</table>

Based on this outcome, the results from the search of 2015 were used. However, it was discovered later that the contributions were not directly related to Mexico concerning the ISPS Code, but rather connecting the country to isolated crime cases or drug organizations.

4 RESULTS

As shown in Table 1, the search from June 2015 resulted into 1,801 articles/books, which was reduced to only 194 after examining the titles; these were further reduced to 75 after consideration of abstracts or preface summary, as well as introduction and table of contents in the case of books. Those that were not included in the next stage were clearly related to concepts that had a better fit with a different discipline -or a different context- and did not comply with the specific combination. The literature review from an author-centric approach is presented in Table III which follows next. In accordance with the type of contributions from the results, eight categories were selected to further study the topic and used for developing the literature review. These categories are the following:

- Concept 1= Terrorism (at sea or maritime terrorism).
- Concept 2= Counterterrorism
- Concept 3= Port Facility Security Plan
- Concept 4= International Ship and Port Facility Security Code
- Concept 5= Maritime Security
- Concept 6= Safety
- Concept 7= Oil Spill & Environmental Protection
- Concept 8= Resilience plan –In the sense of prevention & response & to emergencies (preventive and reactive measures to emergencies)

As it can be observed in table III that follows, in various research efforts (mostly books), the focus includes the analysis of different concepts in relation to the eight categories selected above. A significant number of books focused on port and maritime security, addressing the ISPS Code and PFSP. However, it is noteworthy that safety issues, as a result of security incidents were also addressed in these books. Within this category, the issue most commonly identified was marine pollution caused by

---

<sup>2</sup> In addition to two counted and repeated in CRC-net database.

<sup>1</sup> Mexico, terrorismo, instalaciones portuarias petroleras, plan de protección.
oil spill associated with security incidents. The complete list of the references related to these research items is presented in Appendix I.

Table 3. Author-centric literature review

<table>
<thead>
<tr>
<th>Author</th>
<th>Type</th>
<th>Methods</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Schulz, 2011)</td>
<td>CH</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Pilewski &amp; Pilewski, 2012)</td>
<td>CH</td>
<td>Book</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Norman, 2012)</td>
<td>CH</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Holz, Dudonis, &amp; Schulz, 2012)</td>
<td>CH</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Hesterman, 2013)</td>
<td>CH</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Doro-on, 2014)</td>
<td>CH</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Perdikaris, 2014)</td>
<td>CH</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Kenneth, 2009)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (T. &amp; Tweedy, 2014)</td>
<td>Book</td>
<td>Book</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Espin-Digon, Burns-Herbert, &amp; Bateman, 2008)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Badiru &amp; Racz, 2013)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Rogers, 2007)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Neumann, 2013)</td>
<td>Book</td>
<td>Book</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Pinkowski, 2008)</td>
<td>Book</td>
<td>Book</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Mythen, 2014)</td>
<td>CH</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Litchman, Maharaj, &amp; Waddah, 2012)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Bahr, 2014)</td>
<td>Book</td>
<td>Book</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Park, 2013)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Theodore &amp; Dupont, 2012)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (Spurgin, 2009)</td>
<td>Book</td>
<td>Book</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Cullen &amp; Berube, 2012)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Klein, Rothwell, &amp; Mossop, 2009)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Tuerk, 2012)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Weintrit &amp; Neumann, 2013)</td>
<td>Book</td>
<td>Book</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Bragdon, 2008)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Tanaka, 2012)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Martinez Gutierrez, 2009)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Weinrit &amp; Adam, 2009)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Tan, 2005)</td>
<td>Book</td>
<td>Book</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (Ringbom, 2007)</td>
<td>Book</td>
<td>Book</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 (Papa, July)</td>
<td>Article</td>
<td>Comparative Approach/ Doc. Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 (Jaradat &amp; Keating, 2014)</td>
<td>Article</td>
<td>Literature review and conceptual analysis of “critical infrastructure”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 (Lichterman, 1999)</td>
<td>Article</td>
<td>Reflective analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 (Pierre-Cambacèdes &amp; Bouissou, 2013)</td>
<td>Article</td>
<td>Literature Review Cross conceptual analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 (Phillips, 2008)</td>
<td>CH</td>
<td>Terror Attack Identification &amp; Analysis</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 (Aronica, Mukhtyar, &amp; Coon, 2001)</td>
<td>Article</td>
<td>Analysis of case law.</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 (Mugurara, 2014)</td>
<td>Article</td>
<td>Qualitative. Secondary Data Analysis.</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 (Goede, 2013)</td>
<td>Article</td>
<td>Qualitative. Exploratory comparative case analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 (Haynes, 2000)</td>
<td>Article</td>
<td>Qualitative Comparative case analysis</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 (Holt &amp; McAleer, 2005)</td>
<td>CH</td>
<td>Apply Risk Assessment model to evaluate security of 120 countries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 (Singha, Bellerby, &amp; Trieschmann, 2012)</td>
<td>Article</td>
<td>Use Nmap and Nessus to test network vulnerabilities in offshore In 7 countries.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 (Middleton, Glosec Ltd., Day, &amp; Lallie, 2012)</td>
<td>Article</td>
<td>Magazine article</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 (Crook, 2010)</td>
<td>Article</td>
<td>Risk Analysis on Natural and Human-caused Threats</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 (Giro, 2010)</td>
<td>Article</td>
<td>Qualitative; interpretative methodology with Activity Theory as a conceptual framework</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 (Ibrahim &amp; Allen, 2012)</td>
<td>Article</td>
<td>Qualitative literature review with a comparative approach for three borderlands</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 (Gregory, 2011)</td>
<td>CH</td>
<td>Analysis on International Threats</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 (Fabiano, 2012)</td>
<td>Article</td>
<td>Multidimensional Risk Analysis on Terrorism</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

14 Number corresponding to database
15 Pages: 4, 164, 307, 311, 323.
16 Repeated in ProQuest
17 Repeated and fully available at ProQuest
18 Critical oil infrastructure.
19 Safety and security in several disciplines
20 Organized Crime.
Table 4. Concept Matrix

<table>
<thead>
<tr>
<th>Concept</th>
<th>Articles included in the analysis</th>
<th>Books included in the analysis</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Terrorism (at sea or maritime terrorism)</td>
<td>14</td>
<td>27</td>
<td>41</td>
</tr>
<tr>
<td>2. Counterterrorism</td>
<td>2</td>
<td>15</td>
<td>17</td>
</tr>
<tr>
<td>3. Port Facility Security Plan</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>5. Maritime Security</td>
<td>16</td>
<td>19</td>
<td>35</td>
</tr>
<tr>
<td>6. Safety</td>
<td>1</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>7. Oil Spill &amp; Environmental Protection</td>
<td>4</td>
<td>9</td>
<td>13</td>
</tr>
<tr>
<td>8. Resilience plan</td>
<td>5</td>
<td>20</td>
<td>25</td>
</tr>
</tbody>
</table>

Table 5. Geographic dimension of selected literature

Kenneth (2009). This book is mainly about maritime security in the US, however the author also analyses several maritime security incidents in other countries and devoted some chapters to the study of maritime security worldwide from a historical perspective, written in English. **North-America: United States, Mexico. Central and South America: Brazil, Peru, Ecuador, Chile. Europe: United Kingdom, Greek, Portugal, Spain, Denmark, Germany, Italy, Mediterranean Sea, Greece, France, Turkey. Asia: Indonesia, Malacca Strait, Bangladesh, India, Pakistan, Sri Lanka, Yemen, Iran, Iraq, the Red Sea and Arabian Sea, Suez Canal, Singapore, Thailand, Malaysia, India, Japan. Africa: Nigeria, Somalia, Egypt, Eritrea, Namibia, Senegal, Liberia, Guinea, Angola, Sierra Leone, South Africa**

Espin-Digon, Burns-Herbert, & Bateman (2008). Editors of a book that encompasses several scientific articles related to maritime security & implementation and compliance of the ISPS Code from 31 authors. Note: It does not necessarily means that each of the countries listed are related to a specific study, but often security incidents at some countries are referred to in the study of another one, written in English. **North-America: United States, Canada & Mexico, (This last one was briefly commented in an article addressing drug trafficking). Central and South America: Argentina, Venezuela, Colombia & the Caribbean Sea. Europe: England, Germany, France & Italy, Spain, Italy, United Kingdom, Netherlands and Mediterranean Sea, Asia: North Indian Sea, Red Sea, Arabian Sea, Arabian Gulf and Malacca Strait Singapore, Indonesia, Philippines, Myanmar, Bangladesh, Thailand, Japan, China, South Korea, India, Bangladesh, Pakistan, Sri Lanka, Malaysia, Laos, Vietnam, Kuwait, Yemen, Iraq, East Timor, Suez Canal. Africa: Somalia, Morocco, Egypt, Nigeria & Algeria. Oceania: Australia & New Zealand**

Vaggelas & N (2012). Article with a comparative study about the implementation of the ISPS Code between the Piraeus and Hong Kong ports. **North-America: United States. Europe: Piraeus, Greece. European Union’s implementation of IMO instruments. Asia: Hong Kong, China**

Maldonado (2009). This is an article on operative safety and security related to foreign trade in Mexico, written in Spanish. **North-America: Mexico, United States.**
In order to make the conversion from the author-centric approach towards the category-centric approach and synthesize the relevant literature, table 4 that follows is providing a summary of a category matrix in relation to the number of articles and/or books that were identified during the search.

Then, the items that included in their analysis the categories three, four and five “Port Facility Security Plan; International Ship and Port Facility Security Code and; Maritime Security” were further studied under a geographical dimension, including five subcategories that covered North-America, Central and South America, Europe, Asia and Africa. The complete details of this analysis are illustrated in Table 5.

5 DISCUSSION

The original purpose of this review, which was to examine the state of the art of implementation and compliance of the ISPS Code in México, had to be adjusted since there was only one article that met the search criteria; and which actually falls outside the framework of this literature review, as it is about military law. The results about this objective are clear: the state of the art concerning implementation and compliance of ISPS Code in Mexico is quite poor. The topic really need to be researched and, in general, it is observed that research within the maritime domain in Mexico is limited. Even when it was used some subcategories to get a wider number of research items, it is discovered that those academic efforts that mention Mexico, they do it in a connection to isolated cases of drug organization, proliferation of crime or smuggling of drugs and weapons, but not in direct connection to compliance of the ISPS Code in Mexico. Yet, the research contributions were deeper explored and divided into geographical areas to examine their allusions to the country in the analysis and studied according to eight selected categories, it make it more evident the lack of research in the maritime real in the referred nation. In a previous study Nordfield-Avila-Zúñiga & Dalaklis (2018) have already addressed “the necessity of the inclusion of maritime security and protection of critical oil infrastructure offshore of Mexico in the national agenda that would provide for future research directions in the maritime security domain and contribute to the establishment of a national maritime security policy”.

Therefore, at this stage of the study the scope gets another dimension, since even the search queries were conditioned to the word of Mexico, the research items that have brought connections to this country were for isolated cases, and the contributions that were found are mainly addressed to other parts of the world. Thus, the discussion shifts focus to the eight selected categories; based on the contributions on general bases, rather than the country.

Even though the concept of “terrorism” has been discussed by several authors in the past, there is not a sole definition. Tuerk (2012) pointed out that there is not an authoritative definition of this term, but that all definitions have several features in common: “first, there must be actual or threatened violence; second a political motive is necessary; finally, the acts must be directed at and intended to influence a targeted audience”. To emphasize this, the author cites to note 393, from Power, Maritime Terrorism: “A new Challenge” and further explains that the overall side of the common aspect is arguably that an act is not terrorism unless it has a deliberate political motive. Kenneth (2009) coincides with Tuerk that there are many definitions of terrorism and says that it is simply “the use of force or violence against people and places to intimidate and/or coerce a government, its citizens, or any segment thereof for political or social goals”. The author expands his explanation by arguing that terrorists try to coerce the adversary to obtain a goal without having to face the risk of a direct confrontation, fighting an asymmetrical war, which is an strategy used by the weaker side in the conflict to compensate for the strengths of the enemy.

Espin-Digon, Burns-Herbert, & Bateman (2008), have similar views to the above mentioned authors. They further discuss maritime terrorism21, by arguing that despite the hysteria surrounding, acts of maritime terrorism are by no means frequent, because maritime terrorism requires a certain degree of familiarity with the sea. These researchers also noted that “terrorists would also need a kind of maritime domain awareness (MDA) to even think about including maritime attacks into their modus operandi—and the availability of a special set of knowledge and skills”. Even so, they correctly pointed out that acts of maritime terrorism targeting ships, ports and oil terminals occur and that therefore it is necessary to be prepared with appropriate countermeasures. Kenneth (2009) defines “counterterrorism” in his glossary, as “offensive strategies, tactics and plans used by government agencies, military forces, law enforcement agencies, and private sector organizations to mitigate the threat of terrorism by reducing the chances that individuals or groups can successfully wage campaigns of terror in pursuit of their organizational goals”. Finally, in the context of maritime terrorism and maritime security, discussed by Klein, Rothwell, & Mossop, (2009), counterterrorism may be understood as the capacity of a state to respond to sudden and unanticipated threats.

---

21 Terrorism at sea or terror actions against vessels, port and off-shore installations.
Counterterrorism capacity is one of the objectives of any PFSP, which is an instrument embodied in the ISPS Code to ensure the application of security measures deliberated to protect the port facility and its serving vessels, their cargoes, and persons on board at the respective security levels. According to Kenneth (2009), a port facility is required to “plan and effect security at the levels identified in the risk assessment process and as established by the governmental entities with statutory responsibilities for port security oversight”. This author also emphasized the need of standardizing the terms used in the plan since a term like security, for instance, may have a different meaning for different people in different environments. For the purposes of developing a port facility security plan, he correctly identified that a working understanding of the security should include a set of measures aimed to:

- “Neutralizing vulnerabilities for criminal activity within the port,
- Identifying and responding to safety issues,
- Minimizing the threat of terrorism,
- Reducing opportunities for internal criminal conspiracies,
- Disrupting links between corruption, terrorism and organized crime,
- Sharing intelligence and investigative information, with appropriate law enforcement agencies,
- Promoting opportunities for the exchange of best practices in port security”.

Kenneth (2009) criticised that very often the PFSP exists only in paper, but it is rarely tested for effectiveness and emphasized that “the key to successful port security management in terms of the PFSP is to understand it as a living document”. Vaggelas & Ng (2012), noted that based on the requirements of the PFSA (Port Facility Security Assessment), a PFSP has to be developed for each facility which has provisions for addressing changing security levels for every security operation and that a PFSP may cover more than one facility only provided that the operator, location, operation, equipment and design of those facilities are very similar to each other.

As mentioned before, the PFSP is a requirement of the International Ship and Port Facility Security Code (ISPS Code), which came into force on July 1st. of 2004 and it is a part of the amendments to the 1974 Convention for the Safety of Life at Sea (SOLAS). Kenneth (2009) defined the ISPS Code in his glossary, as the “comprehensive set of measures implemented in 2004 to enhance the security of ships and port facilities, developed and agreed to by member countries of the International Maritime Organization in response to the perceived threats to ships and port facilities after the September 11, 2001, terrorist attacks in the United States”.

Vaggelas & Ng (2012) simplify that the Code has mainly two major components: part A that illustrates the minimum mandatory requirements that ships (represented by their firms) and ports (represented by the contracting government) must follow; while Part B provides more detailed, but not compulsory, guidelines for the implementation of security assessments and plans.

For Espin-Digon, Burns-Herbert, & Bateman (2008), the ISPS Code is a security regime formulated under the auspices of the IMO to strengthen the maritime security in general, and prevent and suppress acts of terrorism against the maritime realm. These authors clarify that passenger ships, including high-speed passenger craft, cargo ships of 500 gross tonnage and above, Mobile Offshore Drilling Units (MODUs) and all port facilities serving ships engaged in international voyages are required to comply with the ISPS Code, according to the established in the SOLAS Chapter XI-2. They also correctly identified that the ISPS aim is to provide a standardized consistent framework for evaluating risk, enabling governments to offset according to changes in different threat levels affecting the vulnerability of vessels, port and offshore facilities.

Furthermore, in an article written by J. Urbansky, W. Morgas and M. Miesikowsky (2009) included in the book edited by Weintritt A. (2009), the authors stated that maritime security is "the security from the terrorism, piracy and similar threats, as well as effective interdiction of all the illicit activities on sea, such as pollution of the marine environment; illegal exploitation of sea resources; illegal immigration; smuggling the drugs, persons, weapons and other matters that can be used for terrorist activities”. All the above also explain why concepts number 1 and 5 are the ones most commonly presented in the research items, since interest on the issue of terrorism and the respective maritime security framework is high. On the other hand, concepts 3 and 4 are rather low in representation. This translates into the fact that implementation issues and related practicalities are clearly lagging behind.

On a different direction, but in similarity to the term of maritime security, there is not a sole and universal definition for the concept of maritime safety, although concepts such as protection of life and property at sea, risk assessment and prevention of hazards are standing out. Piétre-Cambacédès & Bouissou (2013, p.111-112), analysed the similarities and differences between the two domains, safety and security. The authors pointed out that while security is connected to risks originated or exacerbated by a malicious action, independently from the nature of the related consequence, the concept of safety is linked to accidental actions i.e. without a malicious intention, but with potential impact to the related environment. They further clarify that in the security discipline it is common the use of the term threat, while in the safety discipline the tendency is to use the term hazard, even though they are used to describe identical concepts in several standards. An example provided by these authors is the use of the term incident, as an event with minor consequences in safety, while it means an infringement or breach with regards to security.

On this context, Kenneth (2009 p.223-224) cited the U.S. Department of Labor 2001 par.2, to emphasize that: “The core function of any work place safety and health program is to find and fix’ hazards that endanger employees and to implement systems, procedures and processes that prevent hazards from recurring or being introduced into the work place. This element of a worker protection program has the most immediate and direct effect on injury and illness prevention”. The author also noted that port facilities present some unique and extraordinary challenges with respect to safety management because of the variation of operations and its interaction with the vessels, cargo and land-based people, as well as conveyances.
The issue of marine oil pollution is also considered a part of maritime safety and maritime security and it is included in the standards of training and certification as an important part of oil spill prevention. It is addressed as a possible consequence of security incidents. Oil spill has also been addressed several times within maritime security regarding possible terror scenarios. Espin-Digon, Burns-Herbert, & Bateman (2008 p.57), argue that one of the considered terror scenarios in United States is the floating bomb scenario, “that is, a hijacked liquefied petroleum gas (LPG) or liquefied natural gas (LNG) tanker driven into a major port and exploded there, with the intent of disrupting seaborne global trade”. The authors also refer to the “momentum weapon” scenario, which is about a large ship such as an ultra-large crude carrier or a chemical tanker, where the terrorists would attempt to drive the vessel into the harbour at a high speed to ram either other ships with vulnerable cargoes or oil terminals and similar and then detonate the ship. The last cited authors clarify that even if such scenarios as the called “momentum weapon” has been developed, for the port of Singapore, where the largest of Southeast Asia’s oil refineries is located, all of them belong to the realm of fiction. However, it is necessary to be prepared to respond to large terror attacks at port and offshore installations and to mitigate eventual oil spills, protecting the marine environment. It is therefore no coincidence that concepts number 6 and 7 are represented in 18 and 13 occurrences respectively. The fact that there is a rather close correlation in these two numbers is attributed to the fact that oil pollution is widely considered nowadays as the main safety risk.

Regarding resilience’s plans, also known as emergency management plans, Kenneth (2009) refers to the National Response Framework from the U.S., and affirms that this document defines the principles, roles, and structures that frame how the United States will respond collectively in terms of a “national response doctrine” of coordination, specific authorities, and best practices. By citing to U.S. Department of Homeland Security (2008), the author points out that the National Response Framework establishes five key principles that reflect the overarching approach to incident and emergency response, which are: first, engaged partnerships; second, a tiered response; third, scalable, flexible, and adaptable operational capabilities; fourth, unity of effort through unified command; and fifth, readiness to act. He further explains that when developing port specific emergency operations and response policies and procedures; port security managers must take into consideration that each facility plan would be a component of the larger national plan and stresses that “planning for emergency must be managed collaboratively with those port users and government agencies that have interests and concerns in the stability of the port environment”. He further added that it is imperative to have a coordinated response to port incidents (including hazardous materials incidents) and emergencies; additionally, to ensure that these events will be managed competently and in concert with national security priorities. As a result, the total number of occurrences for concept 7 is convincing, since potential safety risks must be addressed via the “right” resilience plans.

6 CONCLUSIONS

The results about the state of the art concerning implementation and compliance of ISPS Code in Mexico are clearly poor. The subject should be further studied and, in general, it is observed that academic contributions within the maritime domain in Mexico are quite limited. The lack of research in the maritime realm in the referred nation might have a connection to the constricted attention of the issue in the national agenda, which then again, is possibly related to the absence of a national maritime security policy in Mexico. Concerning the wider domain of maritime security at ports and offshore installations encompasses directly or indirectly all the concepts included of table IV. However, even if they are considered as different concepts, they cannot be seen as isolated, because in one way or another they are interdependent of each other. Furthermore, safety and security issues can be highly interdependent and also influencing one the other at the same time. In a similar direction, the same interdependency could be argued between oil spill and environmental protection; on the positive side, resilience’s plans (also called emergency management plans) can provide the necessary mitigation toolbox.

Likewise, the concepts of terrorism and counterterrorism are (directly or indirectly) related to both the maritime safety and security domains, because of the severe consequences that are resulted from a successful attack as well as the need the necessary detailed preparation to avoid these “unpleasant events”. In any case, these are various important concepts addressed via the International Ship and Port Facility Security Code (the ISPS Code), which establishes guidelines and recommendations for the development of the Port Facility Security Plan (PFSP). In the long run, the ISPS is a toolbox that sets out processes and procedures to cope with the risks within the maritime security domain.

As it can be seen in the concept matrix, the category of “terrorism at sea or maritime terrorism” was the most studied according to findings of this literature review, with 41 different articles or books examining this topic; the topic of maritime security followed with 35 instances. The fact that “terrorism” and “maritime security” were most commonly presented in the research items could be attributed to the recent terror attack threats worldwide, a situation that has brought global interest on the issue of terrorism at sea and the respective maritime security framework for managing the risk of maritime terrorism and improve maritime and port security.

As already highlighted, the most important set of regulations addressing that subject is the Chapter XI-2 of the Safety of Life at Sea Convention 1974 (SOLAS Convention), encompassing the ISPS Code; this Code requires the establishment of PFSPs at port facilities with specific characteristics. It is also noteworthy that studies approaching the categories concerning the ISPS code and PFSPs were the lowest represented, with only six instances. This can be interpreted into the notion that ISPS Code implementation issues and related practicalities are still worldwide lagging behind in terms of investigation and examination.
As it has been demonstrated in this literature review, research efforts focused on the ISPS Code and the development of a Port Facility Security Plan (PFSP) have an integrated perspective, where the concepts of terrorism and counterterrorism, as well as maritime security management and the issue of port security have a strong interaction and dominant status. Additionally, the safety issue is quite often addressed, with oil spill and environmental protection being included in the consequences of security incidents. Closing with a positive note, after a total of fourteen (14) years after the approval and implementation of the ISPS Code, there have been identified quite a few different approaches to security risk assessment methodologies as it can be observed through the current literature review. On the other hand, more emphasis on the implementation issues of the ISPS Code is evidently needed to ensure that apart from theory, field results are resulting into an acceptable security risk level.

REFERENCES


REFERENCES APPENDIX I


Johnsen, S., Lundteigen, M., Fartum, H., & Monsen, J. (u.d.). Identification and reduction of risks in remote operations of offshore oil and gas installations. SINTEF.


Opening of offshore oil business in Mexico and associated framework to cope with potential maritime security threats

Avila-Zuñiga-Nordfjeld, Adriana
Dalakis, Dimitrios

Opening of Offshore Oil Business in Mexico and Associated Framework to Cope with Potential Maritime Security Threats

A. Ávila-Zúñiga-Nordfjeld & D. Dalakis
World Maritime University, Malmö, Sweden

ABSTRACT: After 75 years of State oil monopoly, Mexico performed the first business oil round in 2015 involving the private sector. This auction-round offered 14 oil exploration fields located on the continental shelf to private companies. The development and exploitation of these hydrocarbon fields faces significant challenges regarding security. The economic loss for theft of hydrocarbons through illegal connections to pipelines is estimated to 973 million, 125 thousand U.S. dollar, only for the year of 2014. While productive research has been made, it has mainly focused on transportation systems and basically, pipelines. The development and establishment of policies prioritizing maritime security and protection of critical offshore infrastructure against theft of hydrocarbons, drugs organizations and terror attacks needs to be included in the national agenda to improve maritime security and mitigate potential security threats at sea, including damage to the marine environment. This could increase the trust of investors and stakeholders and would contribute to the faster development of new exploration and production fields. While the International Ship and Port Facility Security Code (ISPS Code) is the cornerstone for the construction of the port’s security program and establishes the requirements of the Port Facility Security Plan (PFSP), including oil port facilities, it has not been fully implemented in several important Mexican ports. It is concluded that some important ports lack many of the core security processes, procedures and controls that should be included in any PFSP. This article briefly reviews the situation of the oil industry from a security perspective and discusses key elements of maritime security; addressing the necessity of the inclusion of maritime security and protection of critical oil infrastructure offshore in the national agenda that would provide for future research directions in the maritime security domain and contribute to the establishment of a national maritime security policy.

1 INTRODUCTION

Mexico amended its Constitution and energy law to open the oil industry to the private sector. This was a priority for the actual government because since 2008 the government of the United States of America started to lease blocks close to the border line, where the bi-national oil reservoirs from the “Perdido Folt Belt” are located and in consideration to the USA Rule of Capture; pursuant to, “the owner of an area of land acquires title to the minerals produced from wells drilled thereon, even if it is proved that part of such minerals migrated from adjoining lands. This is known in the oil industry as the straw effect.” (Avila, 2008).

On August 12th 2014 the new Hydrocarbons Law and the new Hydrocarbons Revenues Law became effective. These are part of a set of new laws and legal amendments to implement the Constitutional Energy Reform that became effective on December 21st 2013. After 75 years of monopoly in the oil industry; the
country performed the first oil business round and offered 14 oil exploration fields located on the continental shelf to private companies. Whereas, this first round was not as successful as it was expected by the Mexican Government and only two bids were received by international companies for a total of 14 blocks; in the round one second tender the National Hydrocarbons Commission of Mexico (CNH) awarded three of five shallow-water blocks (Comisión Nacional de Hidrocarburos, 2015).

Diverse factors may affect the interest of international investors in the oil industry in Mexico when participating in the oil fields blocks auctions, like the low international oil prices during the last two years or the fact that the first offer was of exploration fields while the second one was of production fields, which gives more security over the investment.

However, another factor that may affect the interest of international oil companies is the security of the oil installations both onshore and offshore. A total of 4 thousand, 298 illegal connections to pipelines have been discovered by Pemex and authorities during the period of January 1st. to October 27th. 2015.

Even though the security challenges in the oil industry are by now more evident ashore, it is necessary to include maritime security in the national agenda as well.

The development and establishment of policies that enhance maritime security and the protection of offshore installations would increase the trust of international investors in the national oil industry.

Maritime security is a topic that has been discussed for several decades at the International Maritime Organization, yet some significant issues remain in discussion and unsolved. The focus of extensive research regarding maritime security has been on piracy at sea, while terrorism at offshore installations, port maritime security and protection of critical infrastructure has not got the same attention.

The International Ship and Port Facility Security Code (ISPS Code) was implemented in Mexico since it entered into force on 1st. of July, 2004, following the requirements and recommendations of the International Maritime Organization. Nonetheless, some of the most important ports of Mexico have not fully implemented the ISPS Code yet. A set of information that according to the requirements of the ISPS Code all the port and port facilities are obligated to keep in logs was missing when such information was requested to the port authorities through the National Institute of Access to Public Information, which reveals a difference between the formal statements of the port regarding the security program purpose and the actual implementation of the ISPS Code. This puts in evidence the urgency of the review of national policies and national legislation in order to enhance maritime security both, at the port and at sea.

2 METHODOLOGY

For the purposes of this study the authors have used the method of document review to analyse the actual situation of the oil industry in Mexico from the security perspective. The data was gathered from different sources that included official information from Petróleos Mexicanos (Pemex), the Mexican oil agency and different authorities published on their webpages. In addition some relevant information was requested to Pemex and other different institutions through the National Institute of Transparency, Access to the Information and Protection of Personal Data (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en Spanish, and represented with the acronym INAI). Once the documents relevant for this topic were gathered, they were further selected and classified according to their relevance to analyse what the security challenges of the oil industry in Mexico are from a strict security perspective.

3 OBJECTIVES

The objective of this paper is to review the situation of the oil industry in Mexico from a security perspective and discuss key elements of port and maritime security; addressing the necessity of the inclusion of port and maritime security and the protection of critical oil infrastructure located in the Continental Shelf in the national agenda, which would provide for future research directions in the maritime security domain and contribute to the establishment of a national maritime security policy.

4 RESULTS & GENERAL DISCUSSION

The security of the oil industry in Mexico has been seriously affected during the last years, which has left significant not only loss of civilian life, but also huge economic losses to Pemex, the Mexican government and the Mexican society as a hole.

The results of this document analysis show that there is an inconsistency between the requirements of the ISPS Code and its actual implementation at some of the most important ports with oil facilities. These factors need to be improved to enhance maritime security and to avoid serious security deficiencies that could result in loss of life, oil spill and environmental damage. Other important security challenges for the oil industry, like the increasing tendency of theft of hydrocarbons were also found.

On September 19th. 2014, the general director of Petróleos Mexicanos (Pemex), Emilio Lozoya Austin, presented the problematic and challenges of Pemex, before the Commission of Energy of the LXII Legislature-group of the National Congress (Parliament). In this presentation, the mentioned director of Pemex said that “In the year 2014, up to August, it is estimated that the volume of crude oil subtracted trough illegal connections to pipelines amounted to 7.5 million barrels, which equivalent cost is 15 thousand, 300 million pesos. That is what is
stolen to the Mexican Government, at least up to this presentation”.

The textual wording in Spanish of the director of Pemex is as follows: “En el mes de agosto se estima que el volumen de combustible sustraído ilícitamente a través de las tomas clandestinas ascendió a 7.5 millones de barriles, con un costo equivalente a 15 mil 300 millones de pesos. Eso es lo que le roban al Estado mexicano o, por lo menos, a la presentación del informe”.

According to the figures published by the National Institute for Statistics, Geography and Informatics the annual average of oil prices for 2014 is 86.5 USA Dollars per barrel, whereas the average for 2015 and up to September that year, the oil price average is 46.6, as figures illustrated in table I.

Table 1. Oil Price Indices per Barrel (Mexico), 2014-2015. Source: Elaborated with data from the National Institute for Statistics, Geography and Informatics (INEGI); price indices series.

<table>
<thead>
<tr>
<th>Period</th>
<th>Price Oil Barrel</th>
<th>Annual Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014/01</td>
<td>90.65</td>
<td>86.5</td>
</tr>
<tr>
<td>2014/02</td>
<td>93.09</td>
<td></td>
</tr>
<tr>
<td>2014/03</td>
<td>93.48</td>
<td></td>
</tr>
<tr>
<td>2014/04</td>
<td>95.68</td>
<td></td>
</tr>
<tr>
<td>2014/05</td>
<td>96.79</td>
<td></td>
</tr>
<tr>
<td>2014/06</td>
<td>98.79</td>
<td></td>
</tr>
<tr>
<td>2014/07</td>
<td>94.65</td>
<td>46.6</td>
</tr>
<tr>
<td>2014/08</td>
<td>90.8</td>
<td></td>
</tr>
<tr>
<td>2014/09</td>
<td>85.82</td>
<td></td>
</tr>
<tr>
<td>2014/10</td>
<td>75.23</td>
<td></td>
</tr>
<tr>
<td>2014/11</td>
<td>71.39</td>
<td></td>
</tr>
<tr>
<td>2014/12</td>
<td>52.36</td>
<td></td>
</tr>
<tr>
<td>2015/01</td>
<td>41.7</td>
<td></td>
</tr>
<tr>
<td>2015/02</td>
<td>47.26</td>
<td></td>
</tr>
<tr>
<td>2015/03</td>
<td>47.36</td>
<td></td>
</tr>
<tr>
<td>2015/04</td>
<td>50.69</td>
<td></td>
</tr>
<tr>
<td>2015/05</td>
<td>54.06</td>
<td></td>
</tr>
<tr>
<td>2015/06</td>
<td>53.87</td>
<td></td>
</tr>
<tr>
<td>2015/07</td>
<td>46.56</td>
<td></td>
</tr>
<tr>
<td>2015/08</td>
<td>39.87</td>
<td></td>
</tr>
<tr>
<td>2015/09</td>
<td>38.82</td>
<td></td>
</tr>
</tbody>
</table>

Therefore the estimated number of stolen barrels from January to August, 2014 amounts to 7.5 million barrels; the economic loss amounts to 648 million, 750 thousand US dollars.

With this information the total economic loss caused by theft of hydrocarbons for 2014 may be estimated; considering that 7.5 million barrels from January to August gives a monthly average of 937 thousand 500 barrels; multiplying this figure for 12 months, it gives a total of 11 million, 250 thousand barrels, which can be multiplied by the average price of crude oil barrel for the year 2014; which is 86.5 US Dollars. Therefore the total economic loss for theft of hydrocarbons for the year 2014, for Mexico, can be estimated to 973 million, 125 thousand U.S. dollars.

The total number of illegal connections to pipelines discovered by Pemex and relevant authorities for 2014 was 3 thousand 635, while this figure increased to 4 thousand 298 for 2015 and only up to October 26th. This figure means that the number of illegal connections to pipelines increased with 18.24 per cent from 2014 to 2015, which can be observed in table 2.

Table 2. Nr. of Illegal Connections Discovered by Pemex or Authorities, 2000-2015. Source: SISI12857200255215, from INAI

<table>
<thead>
<tr>
<th>Year</th>
<th>Nr. of Illegal connections discovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>155</td>
</tr>
<tr>
<td>2001</td>
<td>132</td>
</tr>
<tr>
<td>2002</td>
<td>159</td>
</tr>
<tr>
<td>2003</td>
<td>152</td>
</tr>
<tr>
<td>2004</td>
<td>102</td>
</tr>
<tr>
<td>2005</td>
<td>132</td>
</tr>
<tr>
<td>2006</td>
<td>213</td>
</tr>
<tr>
<td>2007</td>
<td>324</td>
</tr>
<tr>
<td>2008</td>
<td>392</td>
</tr>
<tr>
<td>2009</td>
<td>462</td>
</tr>
<tr>
<td>2010</td>
<td>691</td>
</tr>
<tr>
<td>2011</td>
<td>1361</td>
</tr>
<tr>
<td>2012</td>
<td>1635</td>
</tr>
<tr>
<td>2013</td>
<td>2613</td>
</tr>
<tr>
<td>2014</td>
<td>3635</td>
</tr>
<tr>
<td>2015</td>
<td>4298</td>
</tr>
</tbody>
</table>

If this figure is applied to the loss of barrels for 2014; in this case 11 million, 250 thousand barrels, the increase would amount to 2 million 52 thousand oil barrels, giving a total of 13 million 302 thousand oil barrels for the year 2015. If the estimated amount of loss of barrels for 2015, in this case 13 million, 302 thousand barrels is multiplied by the average price of crude oil barrel for the year 2015 (In this case the average was calculated with figures from the period January-September, as presented in table 1); which is 46.5 US Dollars, the estimated economic loss for 2015 amounts to 618 million 543 thousand US Dollar; under the condition that the production remain unchanged and the average loss of barrels per incident remains the same from 2014 to 2015.

The fact that the estimated economic loss caused by theft of hydrocarbons from 2015 is less than the estimated loss for the year 2014, even considering that the number of incidents of illegal connections to pipelines was larger in 2015 than in the previous year; is because the dramatic fall of the oil prices in 2015.

It was requested to Pemex to provide information about how many clandestine connections where found to pipelines, warehouse tankers, oil terminals, refineries and other oil installations, but this classification had not been registered in the files. However, the discovery of such illegal connections to Pemex installations to steal hydrocarbons have resulted in 14 thousand 547 legal claims, only for the period 2006 to 2015, (Pemex unidad de enlace a travez del INAI 2015, SISI 12857200255215) from which a total of 324 persons have become sentenced with a guilty verdict, as observed in table 3.

According to the same document from the INAI, clandestine connections to pipelines and other oil installations have led to explosions, which have caused the death of two civilian and serious injuries to other four persons in 2014, while in 2015 an individual lost his life by the same cause.

The consequences of illegal connections to hydrocarbon’s pipelines have also caused severe damages to the environment polluting diverse rivers
and valleys because of oil spill. During the period of 2006 to 2015 a total of 571 legal claims for oil spill pollution have been presented as illustrated in table 4.

<table>
<thead>
<tr>
<th>Year</th>
<th>Nr. of Persons Convicted</th>
<th>Guilty Verdict</th>
<th>Acquittal Verdict (No Guilty)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>19</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>36</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>55</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>30</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>34</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>35</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>68</td>
<td>69</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>35</td>
<td>46</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>12</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>0</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>324</td>
<td>298</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>Nr. of Legal Claims for Oil Spill Pollution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>130</td>
</tr>
<tr>
<td>2007</td>
<td>101</td>
</tr>
<tr>
<td>2008</td>
<td>65</td>
</tr>
<tr>
<td>2009</td>
<td>52</td>
</tr>
<tr>
<td>2010</td>
<td>24</td>
</tr>
<tr>
<td>2011</td>
<td>46</td>
</tr>
<tr>
<td>2012</td>
<td>46</td>
</tr>
<tr>
<td>2013</td>
<td>25</td>
</tr>
<tr>
<td>2014</td>
<td>54</td>
</tr>
<tr>
<td>2015</td>
<td>18</td>
</tr>
<tr>
<td>Total</td>
<td>571</td>
</tr>
</tbody>
</table>

To connect illegal pipelines to Pemex’s installations network requires a high degree of expertise. Several employees and ex-employees from the Mexican oil agency have been investigated for participating in these crimes against the nation. Information from another document also from the INAI, with register number SISI1857200171515 (2015), establishes that a total of 136 employees from Pemex had been investigated in relation to theft of hydrocarbons, as illustrated in table 5.

<table>
<thead>
<tr>
<th>Year</th>
<th>Nr. of Employees and Ex-employees investigated for theft of hydrocarbons</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>10</td>
</tr>
<tr>
<td>2007</td>
<td>7</td>
</tr>
<tr>
<td>2008</td>
<td>19</td>
</tr>
<tr>
<td>2009</td>
<td>10</td>
</tr>
<tr>
<td>2010</td>
<td>14</td>
</tr>
<tr>
<td>2011</td>
<td>5</td>
</tr>
<tr>
<td>2012</td>
<td>11</td>
</tr>
<tr>
<td>2013</td>
<td>15</td>
</tr>
<tr>
<td>2014</td>
<td>33</td>
</tr>
<tr>
<td>2015</td>
<td>12</td>
</tr>
<tr>
<td>TOTAL</td>
<td>136</td>
</tr>
</tbody>
</table>

Table 6. Pemex’s employees investigated for other crimes, 2006-2015. Source: SISI1857200171515

<table>
<thead>
<tr>
<th>Crime</th>
<th>Nr. of employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possession of Cocaine</td>
<td>9</td>
</tr>
<tr>
<td>Possession of Cannabis</td>
<td>25</td>
</tr>
<tr>
<td>Falsification of company’s card</td>
<td>1</td>
</tr>
<tr>
<td>Possession/bearing of fire weapons</td>
<td>7</td>
</tr>
<tr>
<td>Violence with weapons</td>
<td>8</td>
</tr>
<tr>
<td>Explosion Threat</td>
<td>1</td>
</tr>
<tr>
<td>Theft of production material, ferric material, working tools, machinery, cable, pipes, car parts, cooper and cranes among other Pemex’s property items.</td>
<td>115</td>
</tr>
<tr>
<td>Murder</td>
<td>1</td>
</tr>
<tr>
<td>Kidnapping</td>
<td>2</td>
</tr>
<tr>
<td>Fraud for selling working positions</td>
<td>4</td>
</tr>
<tr>
<td>Improper (unmoral) Behaviour at work</td>
<td>2</td>
</tr>
<tr>
<td>Psychotropic medicine drugs</td>
<td>1</td>
</tr>
<tr>
<td>Stealing other employees properties</td>
<td>4</td>
</tr>
<tr>
<td>Falsification of fuel tickets</td>
<td>1</td>
</tr>
<tr>
<td>Car accident</td>
<td>1</td>
</tr>
<tr>
<td>Fraud</td>
<td>1</td>
</tr>
<tr>
<td>Attack/assault &amp; Violence</td>
<td>2</td>
</tr>
<tr>
<td>Being member of the “Z” narcotic organization</td>
<td>1</td>
</tr>
<tr>
<td>Alcohol at work</td>
<td>3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>189</td>
</tr>
</tbody>
</table>

Pemex also function as the operator of several oil terminals. The crimes made by some employees of Pemex like falsification of the company card put unacceptable risk to the company and measures to stop these actions are essential regarding security, since this type of actions could be required for terror attacks in a terror scenario. On the other hand, crimes like possession of weapons and drugs can lead to serious accidents putting in risk the safety of the personnel; the installations and the marine environment because of oil spill pollution. It is important to mention that even though maritime security and maritime safety are two different concepts, they are directly connected.

Piètre-Cambacédès & Bouissou, (2013) analyses the similarities and differences between the two domains, safety and security. The authors wrote that while security is connected to risks originated or exacerbated by a malicious action, independently from the nature of the related consequence; the concept of safety is linked to accidental actions i.e. without a malicious intention, but with potential impact to the related environment (p.111). They further clarify that in the security discipline it is common to use the term “threat”, while in the safety discipline the tendency is to use the term “hazard”, even though they are used to describe identical concepts in several standards. An example given by the cited authors is the use of the term incident, as an event with minor consequences in safety, while it
means an infringement or breach with regards to security (p.112).

Klein, Rothwell, & Mossop, (2009 p. 242), states that one of the main characteristics of maritime security is that there are two different dimensions in terms of response to external threats faced by a coastal state. The author establishes that the first dimensions is the fact that exists a core set of threats, values and responses, which any state will bring to bear in seeking to secure its maritime security; which is reflected in the national and international outlook of a state, its geographical location and maritime domain, as well as its bilateral and regional relationships. These are factors that even if they may slightly vary over time, they will remain fairly stable. The authors explained that the second dimension is the “evolving and emerging threats to maritime security”. They further clarified that some of those threats could be periodic or temporary, while others may suddenly arise with little or no warning at all. Therefore, planning and organizing maritime security requires not only ongoing attention to the core values of a state, but also the capacity to respond to sudden and totally unexpected threats with diverse scenarios from oil spills to terror or nuclear attacks, as well as transnational crime against the port or offshore installations (Klein, Rothwell, & Mossop, 2009 p. 242-243).

By citing to Ng and Gujar (2008), Vaggelas & Ng, (2012 p.674) established that port security includes all security and counter-terrorism activities within the port’s domain, including the protection of port facilities and the security of the activities during the interaction of the ship with the port.

In an article written by J. Urbansky, W. Morgas and M. Miesikowsky (2009) presented in the book edited by A. Weintrit (2009 p.3), the authors wrote the following about maritime security: “is the security from the terrorism, piracy and similar threats, as well as effective interdiction of all the illicit activities on sea, such as pollution of the marine environment; illegal exploitation of sea resources; illegal immigration; smuggling the drugs, persons, weapons and other matters that can be used for terrorist activities”.

Maritime security regulatory framework encompasses several international conventions like SOLAS 1974 and respective protocols up to date, MARPOL 73/78 with respective protocols, and the SUA convention from 1998 and 2005 with respective protocols, among others. The International Ship and Port Facility Security Code (ISPS Code) came into force on July 1st of 2004 and it is a part of the amendments to the 1974 Convention for the Safety of Life at Sea (SOLAS). The amendments to the SOLAS Convention included a new chapter XI-2, about special measures to enhance maritime security. Kenneth (2009) defines the ISPS Code as the comprehensive set of measures implemented in 2004 to enhance the security of ships and port facilities, developed and agreed to by member countries of the International Maritime Organization in response to the perceived threats to ships and port facilities after the September 11, 2001, terrorist attacks in the United States.

Vaggelas & Ng (2012 p.677-678) simplify that the Code has mainly two major components, whereas the first part illustrates the minimum mandatory requirements that ships and ports represented by the contracting government must follow, the second part, which is not compulsory, provides guidelines and recommendations for the implementation of security assessments and plans with more detail. The authors clarify that even if certainly the ISPS Code includes a standardized guidance on maritime security for both, ships and ports, it focuses mainly on how terrorist attacks can be deterred and mitigated, while detailed procedures on how to deal with the consequences of such security events, like crisis management or recovery are not addressed. Resilience plans or plans for crisis management are instruments that should be considered as a part of any security program. By citing Sarathy (2006) Zhang, Payam, & Ekwall (2011) expressed that a system of this type should be “a robust, resilient, and flexible that will require extensive coordination both at national and international levels”. Robustness and resilience are different features. By citing to Husdal (2008), Zhang, Payam, & Ekwall (2011) wrote that whereas resilience is the ability to survive, robustness is the ability to rapidly recuperate the stability.

A security plan must rapidly respond to events that threat scenario from a proactive perspective rather than a reactive. However, it should include a resilience plan to reduce consequences of a terror event in a properly reactive way.

Espin-Digon, Burns-Herbter, & Bateman (2008 p.4), says that passenger ships, including high-speed passenger craft, cargo ships of 500 gross tonnage and above, Mobile Offshore Drilling Units (MODUs) and all port facilities serving ships engaged in international voyages are required to comply with the ISPS Code, according to the established in the SOLAS Chapter XI-2.

The Port Facility Security Plan (PFSP) is a legal instrument embodied in the ISPS Code to ensure the application of security measures to protect the port facility and its serving vessels, their cargoes, and persons on board at the respective security levels. Kenneth (2009 p.99), said that a port facility is required to plan and effect security at the levels identified in the risk assessment process and as established by the governmental entities with statutory responsibilities for port security oversight. The author adds that the development of a PFSP shall include measures aimed to neutralize vulnerabilities for criminal activities within the port; identify and respond to safety matters; minimize the threat of terrorism; reduce opportunities of internal criminal conspiracies; disrupt the connection between corruption, terrorism and organized crime; share intelligent and investigative information, with the respective and correct law enforcement agencies; and promote opportunities for the interchange of best practices in port security (p.100).

Vaggelas & Ng (2012), clarified that based on the requirements of the PFSA (Port Facility Security Assessment), a PFSP must be developed for each port facility which has authorization for changes according to the different security levels for every security operation and highlight that a PFSP may be extended to more than one facility only provided that the
operator, location, operation, equipment and design of those facilities are very similar to each other.

Requirements of the port facility security plan establish a number of security records that must be kept updated as a part of the specific security plan.

Some of the information required to keep in logs was requested to some important ports of Mexico through the INAI. This included the number of oil spills by vessels under operations at the port; number of accidents at the port/port facilities, number of fatalities that resulted in loss of life at the port installations; number of dead and seriously injured persons in accidents at work at the port; number of employees arrested by committing crimes related to their working duties or against the interest of the port and the type of crime. However, the answer was that the port agency does not have such information and it was suggested to further require it to the terminal operator. Since the terminal is directly connected to the operation of the port, the port shall also keep this type of information. This reflects deficiencies in the implementation of the Port Facility Security Plan at the specific ports.

The ISPS establishes that the port and port facilities should keep security records including security threats and incidents; oil spills, changes in the security levels and internal audits and reviews, among others. When the appointed authorities, in this case the Ministry of Communications and Transport, discover deficiencies in the implementation of the PFSP their approach should be at a first stage to advise the port or port facility in correcting the deficiency; the second stage is the persuasion of the port or port facility on the need to correct the deficiency; the third stage is the formal notification of the requirement to correct the deficiency; the next step is the commencement of proceedings to impose sanctions for the failure to correct the deficiency; while the last step is the imposition of sanctions for failing to correct the deficiency, according to the provisions established in the ISPS code (International Maritime Organization, IMO 2012). In case of serious security deficiencies that put in risk the ability of the port or port facility to continue to operate at security levels 1 to 3 the authority is able to suspend or restrict specified activities at a port or port facility and cumulative security failings at a port or port facility could lead to the suspension or withdrawal of the approved Port Facility Security Plan and the respective statement of compliance (IMO, 2012).

Furthermore, once the statement of compliance and approval of the PFSP have been withdrawn, the national authorities can demand completion of a full Port Facility Security Assessment (PFSA) and a revised PFSP before reinstating the approval and statement of compliance (IMO, 2012). Kenneth (2009 p. 116) criticises that very often the PFSP exists only in paper but rarely is tested for its effectiveness. The author emphasizes that the key to achieve a successful port security management in terms of the PFSP is to understand it as a living document. He adds that the PFSP should not be written as a one-time effort, but should really be a working document addressing the security threats twenty-four hours a day, seven days at the week, the whole year.

To avoid that port and port facilities stop the compliance of the PFSP, the government through the Designated Authority shall perform PFSP inspections. The frequency of inspections may be programmed and announced in advance could be totally without warning. Inspections may be performed in connection with the initial, intermediate and renewal verification of the port facility’s Statement of Compliance, investigating a security incident or concerning the assessments of the port facility with the Maritime Security Measures (IMO, 2012). The Government through the Designated Authority has the responsibility to ensure the compliance of the provisions of the ISPS Code, as well as other requirements established in International Conventions from which Mexico is signatory to enhance maritime security.

5 DIRECTIONS FOR FUTURE RESEARCH

Maritime security is an area directly connected to several issues that vary from immigration at sea, to smuggling of drugs, weapons; theft of hydrocarbons; terrorism and piracy. All of these areas have research potential within the context of the case of Mexico. However, the compliance of international conventions and national legislation should be reviewed to ensure that the international obligations of Mexico are properly reflected in national law.

Another area is the examination of the implementation of the ISPS Code in the Mexican ports and port facilities, including case studies from ro-ro terminals, container terminals, chemical terminals and oil terminals. It is also suggested to study the case of Pemex concerning security and safety systems to improve security within the organization and to reduce the theft of hydrocarbons. Research about the penalties for theft of hydrocarbons from a holistic perspective, including the social and environmental aspect is also suggested.

6 CONCLUSIONS & RECOMMENDATIONS

According to the results of this document review, the conclusion is that the oil industry in Mexico faces substantial security challenges. The losses are not limited to economic factors, but also to loss of civilian life and the marine environment.

Even though the oil companies as private entities are responsible for implementing effective security systems within their own property and responsibility areas; national authorities must cooperate to ensure the operation of these business activities and to improve the security of vulnerable infrastructure like pipeline networks, offshore installations and port facilities.

Maritime and port security is an issue that should be included in the national agenda for the development of analytical instruments that should provide the fundamentals for an effective and proactive maritime security program and the establishment of a national maritime security policy.
REFERENCES


Enhancing maritime security in Mexico: Privatization, militarization, or a combination of both?

Avila-Zuñiga-Nordfjeld, Adriana
Dalakis, Dimitrios

CHAPTER 3
Enhancing Maritime Security in Mexico:
Privatization, Militarization, or a combination of both?

Adriana ÁVILA-ZÚÑIGA-NORDFJELD
PhDc Maritime Administration: Law, Policy and Security
World Maritime University, Sweden

Dimitrios DALAKLIS
Assistant Professor, (Safety & Security)
World Maritime University, Sweden

Résumé : La présente analyse examine trois options / solutions différentes que le Mexique a mis en œuvre dans ses ports et ses installations offshore afin d’améliorer le cadre de sécurité maritime du pays et d’assurer le respect du Code international de la sécurité des navires et des installations portuaires (ISPS), privatisation, militarisation et enfin leur combinaison. Les conclusions d’un travail de recherche en cours incluent des incohérences dans les données des dossiers d’incidents de sécurité nécessaires ou même leur absence totale. Les compétences et la formation inadéquates des agents de la sûreté de l’installation portuaire (PFSO) se distinguent également. Une autre question importante était l’utilisation de procédures différentes parmi les ports faisant l’objet d’une enquête pour traiter exactement les mêmes problèmes de sécurité. La conclusion claire est que, après douze ans de mise en œuvre du Code ISPS, le Mexique, qui dirige la Commission portuaire interaméricaine de l’Organisation des États américains (OEA), ne respecte pas les exigences du Code ISPS à un niveau acceptable. L’absence d’une politique nationale de sécurité maritime a entraîné une culture appauvrie de la sécurité maritime, malgré les graves problèmes de sécurité auxquels ce pays est confronté. Il est également vrai que le pays discute actuellement de la réorganisation de son appareil de sécurité maritime, avec des résultats positifs. Des outils et recommandations pour améliorer le cadre opérationnel de la sécurité maritime mexicaine sont donc envisagés, ainsi que les domaines potentiels de recherches futures.

1) p1501@wmu.se
2) dd@wmu.se
Abstract: The current analysis examines three different solutions that Mexico implemented within its ports and offshore installations in order to improve the country’s maritime security framework, as well as ensuring compliance with the International Ship and Port Facility Security Code (ISPS Code): privatisation, militarisation and, finally, their combination. The findings of an on-going research effort include inconsistencies within the data of the necessary security incident records, or even their total absence. Inadequate competence and training among the Port Facility Security Officers (PFSO) also stands out. Another important issue was the use of different procedures among the ports under investigation for dealing with exactly the same security incidents. The clear conclusion is that after twelve years of the ISPS Code implementation, Mexico, which is leading the Interamerican Port's Commission of the Organisation of American States (OAS), does not comply with the requirements of the ISPS Code at an acceptable level; the lack of a national maritime security policy has resulted in a poor (maritime) security culture, despite the severe (security) challenges that this nation is facing. It is also true that the country under discussion is currently reorganising its maritime security apparatus, with some positive results; tools and recommendations for enhancing the Mexican maritime security operating framework are therefore provided, along with areas of potential future research.
III. Enhancing Maritime Security in Mexico: Privatization, Militarization, or ...  

Introduction

After the tragic events of September 11th, 2001, the International Maritime Organisation (IMO) developed a set of maritime security regulations for managing the risk of maritime terrorism, as well as improving security status at sea and the various port locations around the globe. These provisions were established in the new Chapter XI-2 of the Safety of Life at Sea Convention 1974, (SOLAS Convention), comprising the new International Ship and Port Facility Security Code (ISPS Code).

The IMO defines the ISPS Code as "the comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States". Compliance with the ISPS Code and submission of related information to the IMO is not mandatory for all IMO member states, but only for those Contracting Governments to the SOLAS 1974 Convention. However, there is no penalty mechanism in place for states that fail to effectively comply with the ISPS Code. The overall concept is not to impose penalties, but to rely on market forces and economic factors to ensure compliance (official website IMO, SOLAS 1974). However, after 12 years of implementation of the ISPS, market forces and economic factors had not been powerful enough to result in full compliance in Mexico, where serious deficiencies were detected by an on-going research effort.

The SOLAS 1974, Chapter XI-2 establishes special measures to enhance maritime security, while Regulation XI-2/3 of this chapter addresses the ISPS Code. Whereas part A of the Code establishes the mandatory provisions, the not mandatory ("recommended") part B encompasses guidelines about how to comply with the mandatory requirements of part A. This set of regulations only applies to passenger ships, including high speed passenger vessels; cargo vessels of 500 gross tonnage and over; Mobile Offshore Drilling Units (MODUs) in transit and at ports (but not fixed and floating platforms and MODUs on the oil field); and all type of port facilities serving vessels offered for international voyages. In any case, the extent to which the guidelines apply on ships will depend on the type of the ship, its cargo and number of passengers, as well as its sailing routes and the features of the port or port facilities visited by that specific ship. Regarding the application of guidelines to port facilities, it will depend on the type of carriages and vessels visiting that particular facility and its "ordinary" trading routes.

In Mexico there are 16 Federal Integrated Port Administrations (FIPA) where the ISPS Code applies; they are operating under concessions given by the Ministry of Communications and Transport (and called thereafter MCT) and are the following:

3) Administración Integral Portuaria, in Spanish, also known as APIs.
4) Secretaría de Comunicaciones y Transportes in Spanish, and represented with the abbreviation SCT.
Altamira, Tampico, Tuxpan, Veracruz, Coatzacoalcos, Dos Bocas, Progreso, Ensenada, Guaymas, Topolobampo, Mazatlán, Puerto Vallarta, Manzanillo, Lázaro Cárdenas, Salina Cruz and Puerto Madero, (SCT, 2016). The principal requirements of the ISPS Code for ports and port facilities cover the development and implementation of the Port Security Plan (PSP) and Port Facility Security Plan (PFSP) respectively, as well as the designation of the Port Security Officer (PSO) and Port Facility Security Officer (PFSO). Other provisions cover control of compliance with maritime security measures and registration of security incidents.

According to the mandatory Part A of the ISPS Code, contracting governments have to appoint the Designated Authority to carry out certain maritime security duties/responsibilities established in the Code. This Designated Authority holds the responsibility of ensuring compliance with the maritime security measures at all ports (where the ISPS Code apply) through the Port Security Assessment (PSA) and Port Facility Security Assessment (PFSA). The revision, approval and control of compliance of the Port Security Plan (PSP) and Port Facility Security Plan (PFSP), which shall be based upon the PSA and the PFSA, are also included. In Mexico the Designated Authority is the MCT through the General Direction of Merchant Marine (GDMM).5

A very important function within the ISPS code is the setting of security levels, which is performed by governments through the Designated Authority. It focuses on the alert for the perceived risk of terrorist attacks, but governments may include other type of threats in their risk evaluation like pirate-type attacks against vessels and oil platforms, or even the possibility of kidnapping port(s) and terminal(s) personnel. These security levels apply both to ships sailing within the respective territorial sea, as well as into port facilities. The Designated Authority can decide on the implementation of different security levels for different ports, port facilities and different areas of their territorial waters. It is necessary to point out that the change of security levels must be clearly communicated to the associated port(s), port facilities and vessels transiting or attempting to transit those areas (IMO, 2012).

As established by IMO, there are three different security levels, where Security Level 1 is considered normal and requires the minimum appropriate protective security measures at all times. Its priority is the normal conduct of commercial operations and facilitation of trade. Security Level 2 requires additional protective security measures for the specific period of time that the risk of a security incident is heightened. Its priority is the allowance of continued commercial operations, but with increased security measures and its consequent restrictions. Security Level 3 requires specific protective security measures which shall last only for a limited period of time when risk for a security incident is probable or imminent, even when it is not possible to identify the

5) Dirección General de Marina Mercante, in Spanish.
III. Enhancing Maritime Security in Mexico: Privatization, Militarization, or ...

target. It encompasses the strictest security measures and its priority is the security of
the port, port facilities, vessels and society that may be affected by a security incident
and can result even in the suspension of commercial operations.

The control of security response under Level 3 is transferred to the Government or
other organisations responsible for dealing with significant incidents (IMO, 2012). In
Mexico it is the President of the Unified Centre for Port and Maritime Security (hereafter
UCMAR), who is responsible for port security and coordinates all operations under
Level 3. As established by Regulation of the UCMAR published on the Official Diary
of the Federation on 21 April, 2014, provision 6: “a UCMAR shall be established at all
the 16 ports (FIPAs) designed to receive vessels of over 500 gross tonnage”; known as
“Puertos de Altura”, in Spanish. Additionally, provision 8 of this regulation establishes
that it shall be the Commander the Navy Military Zone of each jurisdiction where an
UCMAR is established who shall be the President of that respective UCMAR.

According to the Law of Ports Article 19 SECOND, the UCMAR is a group of
interinstitutional coordination between the Ministry of Marine (hereafter MMAR) and
the MCT for the application of maritime security measures; effective prevention and/or
dealing with security incidents is the aim. Article 19 THIRD, paragraph II of this law
puts forward that the UCMAR shall apply all the terms and response measures within
the framework of the Chapter XI-2 of the SOLAS 1974 Convention, comprising the
ISPS Code and ensures the establishment of a series of functions and actions for
each of the respective three security levels. Also, paragraph III states that the UCMAR
shall function as the coordinator for all actions of the three different levels of government
(municipal, regional and federal) in relation to maritime security.

The key instruments and concepts related to maritime security are addressed in the
ISPS Code, with the aim to ensure security at ports and within an acceptable risk
level. Some of these key instruments are the PSA and PFSA, which encompass the
evaluation of security risks of the port or port facility. This risk evaluation must be
done to develop the PSP or PFSP in the case of terminals, which then must be
approved by the Designated Authority. The PSP is designed to ensure the compliance of
measures and procedures aimed to protect the port, persons, cargo, port equipment
and machinery and the vessels serving or buying services to that port from threats,
security risks, and security incidents. The PFSP has the same objectives as the PSP,
but limited to the terminal. The PSO and PFSO are the bodies responsible for ensuring
that the risk evaluation (PSA/PFSA) is carried out according to the principles and
guidelines of the ISPS Code, submitted and approved; to establish the respective

6) Centro Unificado para la Protección Marítima y Portuaria and represented with the abbreviation «CUMAR» in Spanish.
7) Diario Oficial de la Federación, in Spanish.
8) Secretaría de Marina, represented with the abbreviation «SEMAR» in Spanish.
PSP/PFSP based on its PSA/PFSA and get it approved as well. Once approved, the PSO/PFSO is also responsible for implementing and maintaining (or even improving via formalised procedures) the plan at all times.

Once the Designated Authority performs the necessary inspections to verify the development, implementation and compliance of the PSP/PFSP, it may issue the Statement of Compliance (SOC) for a specific period, which shall not exceed five years, the maximum period of validity. After the SOC is issued, the PSO/PFSO is also responsible for ensuring compliance with the necessary training, exercises and practices; coordinating the inspections in scene in cooperation with the respective authorities; performance of internal security audits and liaison with the Designated Authority’s representatives for external audits. PSO/PFSO must attend security incidents and keep incident security records updated. Security incidents themselves must be considered in the evaluation of risk and integrated into the security plan to achieve a constant reduction of risks and the continuous improvement of port (and maritime) security.

In the case of Mexico, even if the GDMM of the MCT is the Designated Authority responsible for the revision, approval and control of compliance of the PSP(s) and PFSP(s), the UCMAR is co-responsible according to its Regulation, Article 7, paragraph II, which states that: "[UCMAR] shall participate in the evaluation of risks of maritime and port security, previous to the elaboration of the security plans and it shall propose the necessary modifications and updating to those plans". Paragraph III of this article also adds that, once the plan has been approved, the UCMAR shall participate in the verification and control of the compliance of such plans to ensure their effective implementation.

In recent years, Mexico experienced a period of extreme violence, where "extortion payments" were demanded of owners and operators of port terminals, in order not to kill them personally or damage their installations, as denounced by the Federal Deputy from the Deputy Chamber of the Federal Congress, LXII Legislature, Germán Pacheco Díaz, before Parliament, Chamber of Deputies on 5 November 2013. This led to the reorganisation of maritime security in the country, amendments to several laws and the approval of new regulations since 2014, including the Law of Ports, the regulation in relation to the UCMAR, and the Law of Navigation and Maritime Trade, among others. Additionally, the creation of the military navy unit for port security (hereafter NAUPPRO) was decided.

9) «Cobro de Piso» in Spanish.
10) Unidad Naval de Protección Portuaria, represented with the acronym UNAPROP in Spanish.
Research Methodology

The research methodology includes the use of an extended questionnaire with 71 open questions concerning maritime security, sent to eight ports of Mexico; Altamira and Tampico (Tamps.), Tuxpan, Veracruz and Coatzacoalcos (Ver.), Dos Bocas (Tab.), Progresso (Yuc.) and Madero (Chiapas), through the National Institute of Transparency, Access to Information and Protection of Personal Data (called National Institute of Access to Information (NIAI) hereafter). A questionnaire of 70 similar questions (but specifically addressed to oil maritime terminals) was also sent to "Pemex Exploración y Producción" through the NIAI to acquire information for the following terminals: Dos Bocas (Tabasco), Terminal Maritima de Pemex Puerto Isla del Carmen (Camp.), Arbol Grande (Tamps.), and Cobos (Ver.); as well as the following terminals from "Pemex Transformación Industrial": Madero (Tamps.), Tuxpan (Ver.), Pajaritos (Ver.), Guaymas (Son.), Salina Cruz (Oax.), Veracruz (Ver.), Lerma (Camp.), Progreso (Yuc.), Acapulco (Gro.), Lázaro Cárdenas (Mich.), Manzanillo (Col.), Mazatlan (Sin.), Topolobampo (Sin.), La Paz (B.C.S.) and Rosarito (B.C.).

An inquiry into the establishment of the NAUPPRO at the different ports of Mexico was sent to the MMAR, while another request for information about the total number of persons employed at private security companies that have got the courses 18.2 and 18.3 as required in the ISPS Code was sent to the FETNAMM, also through the NIAI. The NIAI was created to comply with the provisions of the General Law of Transparency promulgated in 2012. This law establishes that information from public institutions operating with money from national resources shall be open to public scrutiny with exceptions related to national security. The information delivered through the NIAI is official and publicly available.

These actions were combined with a six-day visit by the researcher to one of Mexico’s three largest ports with oil terminals conducted in April 2016, where she conducted interviews and participant observation. The questionnaire that was sent to the other ports through the NIAI was also answered by respondents at that specific port. Several employees, the PSO and PFSO(s), the Director of the port, the Master of the harbour (referred to as Regional Captainship of the Port in Mexico), the Director of the Port Customs Unit and the Commandant of the maritime police (NAUPPRO) were interviewed. In doing this, the researcher covered the four pillars for the operation of the port. The pool of data is deemed sufficient, based on the fact that nine out of sixteen ports where the ISPS Code applies (representing a coverage of 56% of them

---

11) Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales in Spanish, and represented with the acronym INAI.

12) «Fideicomiso de Formación y Capacitación para el Personal de la Marina Mercante Nacional», and represented with the acronym FIDENA in Spanish, which may be translated to «Fund of Education and Training of the National Merchant Marines», and called FETNAMM thereafter.
and seven out of seven FIPAs situated in the Gulf of Mexico, where oil exploration and production activities take place, covering 100% of them) were included in the study; 100% of Pemex’s terminals are also included, creating valid representation for the case of Mexico (see figure 1).

![Map of Federal Integrated Ports Administrations (FIPA) in Mexico](image)

*Source: The Secretary of Communication and Transportation (SCT)*

Figure 1 Federal Integrated Ports Administrations (FIPA) in Mexico.
(Ministry of Communications and Transport, 2016).

The results from the questionnaire were further analysed through "document analysis" with an exploratory approach, to confirm or reject the inexistence of security incidents at the selected ports and oil terminals in national newspapers and media sources, using Google to have a wider coverage within the period of 2004-2015. Data was classified using codes and categories for the overall analysis to present the results and its respective discussion.

**Results & Findings**

According the results of the questionnaire, six ports and the maritime terminals from both "Pemex Exploración y Producción" and "Pemex Transformación Industrial" have had no security incidents at all in the course of 2010-2015. Furthermore, they officially replied that until now, there has never been any security incident; the seventh port reported that "at least five security incidents of low-impact were registered during the period 2010-2015", while the port of Tuxpan wrote that "they have the antecedent of..."
III. Enhancing Maritime Security in Mexico: Privatization, Militarization, or ...

five maritime incidents, highlighting that it is the duty of the GDMM to classify them as low, middle or high impact*. "Only one" low-impact security incident was registered at the visited port during the same period, following the questionnaire, but the field-findings from the interviews and participant observation at this port proved the existence of at least three security incidents classified as with high impact.

To each of the specific questions about security incidents concerning armed attacks for robbery at the port/port facility; confiscation and smuggling of weapons and drugs or other dangerous restricted substances in the cargo; cargo theft at the port/port facility; theft of material and other items or machinery on the part of employees, property of the port/port facility; personnel working under the effects of drugs and psychotropic substances; situations of vandalism and sabotage; and kidnapping of port/terminal personnel, with the exception of one port, where a weapon was confiscated, the respondents from the other eight ports and Pemex terminals replied that there has never been any security incident of that nature. This significantly differs from the findings of the document analysis through Google, as summarised in tables 1 and 2 respectively.

Table 1 Security Incidents at the Elected Ports

<table>
<thead>
<tr>
<th>Security incident (Ports)</th>
<th>Port</th>
<th>Date</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confiscation of 11,720 kilos of cocaine in a container and arrest of seven persons that were “pro- testing” it. This confiscation of cocaine was the biggest of the Mexican history up to that date.</td>
<td>Tampico</td>
<td>7th October, 2007</td>
<td>JCM, 2007.</td>
</tr>
<tr>
<td>An oceanic patrol ship, confiscated 2,479 kilos of cocaine from the fishing boat &quot;Chara- musca&quot;, which was navigating in the proximity to Port Madero in Chiapas.</td>
<td>Madero</td>
<td>27th April, 2010</td>
<td>SEMAR, 2010.</td>
</tr>
</tbody>
</table>
## Table of Events

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Location</th>
<th>Date</th>
<th>Source(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confiscation of 169 kg. of cocaine in a container downloaded from the ship “Monte Oliva” with German flag.</td>
<td>Altamira</td>
<td>21st September 2015</td>
<td>Letra Roja, El Color de la Información, 2015.</td>
</tr>
<tr>
<td>Confiscation of 15,800 litters of dilute cocaine, from a container unloaded from the ship “Monte Verde” coming from Panama.</td>
<td>Veracruz</td>
<td>1st of March, 2016</td>
<td>Salinas, 2016.</td>
</tr>
<tr>
<td>Confiscation of the fishing vessel “Tuxpan” with 1,800 litres of stolen hydrocarbons. The combustibles had been stolen some days before to another vessel, property of Pemex, which had sailed off from the Port of Dos Bocas, Paraíso, in the Southern state of Tabasco.</td>
<td>Frontera</td>
<td>1st of March, 2016</td>
<td>Ortiz, 2016.</td>
</tr>
<tr>
<td>A kidnapped Pemex’s worker was rescued and liberated by the police.</td>
<td>Altamira</td>
<td>29th July, 2016</td>
<td>Zona de Guerra sin Censura, 2016.</td>
</tr>
<tr>
<td>Extortion Payment was given in order to ensure the life of directors, employees, terminal operators and Pemex’s contractors towards crime ring organizations.</td>
<td>Several Ports and oil terminals.</td>
<td>Several events with reference to period 2010-2013</td>
<td>Cámara de Diputados del H. Congreso de la Unión, LXII Leg., 2013.</td>
</tr>
<tr>
<td>Increase in confiscation of weapons, drugs and stolen hydrocarbons at marine ports with the establishment and activation of UNAPROP(s) and higher participation of the SEMAR in the administration of ports.</td>
<td>Several ports</td>
<td>Several events with reference to period 2010-2013</td>
<td>Cámara de Diputados del H. Congreso de la Unión, LXII Leg., 2013 and Gaviña 2016.</td>
</tr>
</tbody>
</table>
Table 2 Security Incidents at Oil Terminals

<table>
<thead>
<tr>
<th>Security incident (Pemex terminals, Offshore Tabasco)</th>
<th>Terminal</th>
<th>Date</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plundering and dismantling equipment from the (new) platform Yaxche Bravo, including theft of very costly materials.</td>
<td>Yaxche Bravo</td>
<td>15th September, 2008</td>
<td>Pérez, 2010.</td>
</tr>
<tr>
<td>Plundering of the platform Kix-2 where the offenders took even all the navigation lightening signs.</td>
<td>Kix-2</td>
<td>14th October, 2008</td>
<td>Pérez, 2010.</td>
</tr>
<tr>
<td>Plundering of the platform Yaxche Bravo again, stealing the whole heliport. The outcome of this official investigation GPDM-SCO-D8-190-2010, has not been published yet.</td>
<td>Yaxche Bravo</td>
<td>4th May, 2010</td>
<td>Pérez, 2010.</td>
</tr>
<tr>
<td>Kidnapping of several directors and leaders of the worker's union as well as owners of companies giving services to Pemex in different cases (reportage)</td>
<td>Several States</td>
<td>2010-2013</td>
<td>Pérez, Voltairenet.org, 2010.</td>
</tr>
<tr>
<td>Gasoline is stolen inside Pemex</td>
<td>Tuxpan</td>
<td>22nd August, 2016</td>
<td>(Martínez, 2016)</td>
</tr>
</tbody>
</table>

Regarding ships or small boats without the required authorisations to infringe into restricted areas of navigation, the reply from the Port of Tampico was that "the Port Security Plan does not consider any restricted area of navigation and therefore there are not any register about security incidents of such situation". Altamira, Coatzacoalcos, Dos Bocas, Port Progreso and the visited port admitted to having had such situations.
ADRIANA ÁVILA-ZÚÑIGA-NORDFJELD AND DIMITROS DALAKIS

while ports of Tuxpan, Veracruz and Madero as well as all the terminals from Pemex answered that they have not had such situations.

During the field visit of the researcher to the port of interest and travelling towards the open sea on board an oceanic patrol vessel, a small group of boats similar to those commonly used by smugglers was observed; the boats were located just a few meters besides the main sea passage towards the container terminal. Also, this event was noticed while a large container vessel was approaching the port facility: nothing was done to send them away and prevent a dangerous situation. The officials’ reply was that: “they are just fishing; we have taken them off many times before, but they always come back”. Additionally, it was noted that the average time for inspecting persons and vehicles in the access/exit control zones was just 45 seconds, a very short period of time and an indicator of low-quality inspections.

It is also interesting to consider that a small glass containing cannabis was personally noticed at the office of the PFSO from one of the terminals; he said that a few years back, they caught a person from a construction company working inside the port, with about 300 grams of cannabis: “it was like 300 grams and that is not for personal use, but for trade”. The person was forced to resign, but because of time-consuming paperwork related to an official investigation, the case was not brought to court and the PFSO just kept the cannabis in a small glass container with alcohol to cure muscular damage. In an interview to another employee, it was revealed that the Pemex’s oil terminal in the specific port was operating without a formally appointed PFSO since early October 2015 (almost six months before the time of the visit), when the person holding that position had retired.

With personnel from the Navy mastering the harbour since November 2013 and the creation of the NAUPPRO, the status of maritime security improved substantially at the visited port in practical terms. Other measures to improve maritime security were also implemented, such as the use of two different private security companies: one for the operation of the video vigilance system, and the other for control and vigilance of access and exit zones, to avoid security incidents at the control zones being erased from the video records. Security measures were reflected in an increase of confiscation of drugs and dangerous substances, though this improvement in performance was not reflected in incident security records (mismanagement practices prevailed). Last but not least, terminal operators, directors and employees gradually recovered the feeling of safety when the extortion payments from crime-ring organisations disappeared.

Other findings from the questionnaires, as well as other information acquired from the MMAR and the FETNAMM, through the NIAI include the following:

• Different procedures and allocated periods across the country for keeping and maintaining security incident records.
III. Enhancing Maritime Security in Mexico: Privatization, Militarization, or ...

- Inexistence of security incident registers at certain ports and Pemex terminals.
- Failure to classify risks and threats at ports and oil terminals.
- Poor performance of PFSA for the 15 oil terminals of "Pemex Transformación Industrial." PFSA are the fundament of the PFSP, which have not been amended since its original approval in June 2004, despite the incidents reported by the media and a double recertification.
- Wide use of private security companies to perform specific security duties at the ports, whereas Pemex has its own security employees with support from the Navy.
- Misunderstanding of responsibilities and duties on the part of the PSO(s), PFSO(s).
- Lack of awareness of the duty for registering items’ confiscation in incident security logs.
- Establishment and activation of 14 NAUPPROs from September 2014 to August 2015, with an average of 43 elements per unit at fourteen ports, including Altamira Tampico, Tuxpan, Veracruz, Coatzacoalcos, Ciudad del Carmen and Progreso.
- PSO limited training to various elements of the NAUPPRO during the period 2014-2015.
- Arrangement of 369 courses for "personnel of the port/port facility with specific security duties" (18.2 ISPS Code) and 93 courses for "security knowledge that must have the port/port facility personnel" (18.2) by the FETNAMM (established by the Designated Authority); where the total number of participants hired by private security companies amounted to 4,573 and 1,274 respectively, during the period 2010-2015.
- Deficiencies reported from Designated Authority’s audits to some ports covered improving maintenance of security equipment, providing more security training, construction of walls along the port area and reinforcing surveillance and lighting equipment.
- The certificate of compliance with the ISPS and approval of PFSP of two Pemex terminals (Terminal Marítima Árbol Grande and Terminal Marítima de Cobos) were originally issued in 2006 and have not been recertified, but they are under normal operations.
- The certificate of compliance with the ISPS and approval of PFSP for the port of Tuxpan expired in 2014, but is under normal operations during "the recertification process".
- Inadequate performance of Designated Authority’s audits and inspections, since they audited these ports and terminals every year during the period 2010-2015 without reporting serious deficiencies; lack of security incidents records and inadequacy in the classification of security risks.
ADRIANA ÁVILA-ZÚÑIGA-NORDFJELD AND DIMITROS DALAKLIS

• Testing of the "militarisation" model at the visited port, where the port administration and the Regional Captainship of the Harbour were given to personnel from the Navy.
• Improvement of interinstitutional communication and coordination at the visited port.

General Discussion

The situation illustrated in tables 1 and 2 forced the authorities to initiate the reorganisation of maritime security mechanisms in 2013, including justice reforms to provide juridical support to those changes. In addition to traffic of drugs and weapons, theft of hydrocarbons is affecting the economy of Mexico as well as the overall maritime security status. The assessment for theft of hydrocarbons amounted to 11,250,000 barrels, with an estimated economic loss of 973,125,000.00 U.S. dollars, only for 2014 (Nordfjeld & Dalaklis, 2016). Before the NAUPPRO was created in 2014, port security was mainly provided by private security companies, which increased the vulnerability and risk of port installations. Given its political significance related to national security, maritime and port security should be the responsibility of the government and international organisations, covering strategic installations, including offshore platforms. However, the level of security challenges in Mexico relating to a combination of terrorism13, organised crime, marine piracy and poor performance on the part of the Designated Authority, showed that the government was not able to meet its responsibilities and provide satisfactory physical protection to port and oil installations, forcing port administrations to rely on private security companies.

As expressed by Kerr (2010), private security companies can provide a security package quicker than governments because they have less bureaucracy and can operate with a lower profile than most government forces. On the other hand, they are limited by the regulatory framework, concerning the use of firearms and are more exposed to corruption and dispersion of sensitive information as a result of constant personnel rotations, which increases the risk of uncertified employees and poor training standards. Ports included in this research outsourced the "specific security duties" service to private security companies for covering vigilance access control zones, guarding of vigilance towers and inspections of cars and baggage at the access/exit control zones. Terminals have their own security management. On the other hand, Pemex choose to have its own security force for its terminals, with extra support from the Navy when necessary; this resulted into avoiding external worker rotation and the risk of spreading sensitive information concerning security routines.

13) Theft of hydrocarbons and plundering of oil and offshore installations is considered terrorism, following the new Federal Law to Prevent and Sanction Crimes Committed Concerning Hydrocarbons.
III. Enhancing Maritime Security in Mexico: Privatization, Militarization, or ...

Excepting Dos Bocas, and other ports not included in the study where the respective naval unit has not yet been activated, the Navy and the NAUPPRO have taken over the security of strategic installations, including offshore and port facilities. The agreement for the creation of 19 NAUPPROs, which function as maritime police, including duties of vigilance, inspection and control within the port and ocean port roadways, was published on 31 Mars 2014. These units are additional to the elements from private security companies and are responsible for special security duties to detect trafficking of drugs, weapons and other restricted substances during the uploading and downloading operations from vessels as well as the presence of unauthorised persons. This implies a combination of the initially established security management, "privatisation of security services" and definitely some "militarisation".

As expressed by Germán Pacheco Díaz, representative from the national congress (2013), confiscation of drugs and restricted substances in cargo increased in the port of Altamira with the establishment of this maritime police. However, the kidnapping of port personnel and extortion payments to crime ring organisations remained. There are several benefits in the combination of military forces and private security companies, including the economic aspect. Regarding cooperation, private firms need to integrate their operations with relevant stakeholders (such as naval, coastguard, customs and police forces) to reduce the chances of "blue on white" incidents, maximise the opportunities to receive support, and ensure the standards of skills and professional knowledge of its work force (Kerr, 2010). When outsourcing port and maritime security to private security companies, it is still the responsibility and duty of the Designated Authority to conduct periodic and random audits and inspections at the ports to examine the compliance of the PFSP as well as security service providers, to ensure that they have the required certification and security training.

To apply a proper response to maritime security incidents, it is crucial to ensure a regional solution that includes the cooperation of international forces in a specific geographical area if necessary, particularly when the consequences of a maritime security incident will go beyond maritime boundaries, as is the case of oil spill pollution caused by safety and security incidents. As Cordner (2011) points out, major security incidents are likely to have severe environmental consequences that will transcend national boundaries; this highlights the need for government, industry and regional consultative entities to adopt a strategic risk management approach. There is simple explanation why: "No single Agency or jurisdiction currently maintains the capability, capacity or resources necessary to prevent, prepare for, respond to and recover from an armed takeover of an offshore facility. Rather, collaboration with regional partners at the local, state and federal levels ensures that an effective and safe response capability is maintained" (Applegate & Hill, 2014). But, challenges related to a regional solution implies that while strategic plans exist to identify frameworks and guidelines for command and control, they do not operationalise response architecture to implement and sustain coordinated training programmes and integrate planning and resource coordination efforts (Applegate & Hill, 2014).
The government is testing the militarisation model at the visited port where, in addition to private security companies and the NAUPPRO, the Director and the Master of the harbour are Rear Admirals from the Navy, while the President of the UCMAR is the 1st commander and Rear Admiral from that naval zone. The only civil authority in this equation is the Director of the maritime customs unit, who said that the coordination between the authorities and the port has improved substantially since the arrival of the Navy. The respondent added: “At the beginning we didn’t know how it was going to function, if trade would be affected, if it would be closed, but here at this port, the external factor of security improved the trade operations and (...) the coordination is very good; we have systematic security meetings, where all the organisations involved participate.” The original scepticism towards a military discipline on the part of port employees was transformed into a feeling of safety and satisfaction with the military leadership. As a result, the shipping companies recovered the trust to transport their carriages through Mexican ports, as expressed by Francisco Orozco Mendoza, Chairman of the Mexican Association of Shipping Agents,14 Mundo Portuario (2014). The director of the port emphasised that the main risk at the port today is related to hurricanes and stormy weather.

Additionally, during the interview with the Master of the harbour at the visited port, he pointed out that: “why am I working here, even I belong to the Navy? Yes, I am working in another Ministry. Well, in 2013 the insecurity situation at this province continued, especially at the Port. Therefore, the President ordered the MMAR that Naval Officers should be brought in to support and control the port administration and the captainship of the harbour, because the status of security was at a clearly unacceptable level. Criminals even exporting illegally extracted minerals. There was not a security plan for level 3 which should be implemented by the Navy, because in order to create a plan for level 3, there should be measures established for level 1 and level 2 in advance, but that was not achieved.” It is true that Mexico signed the protocols for the ISPS Code, but the MCT did not perform an effective job and many points towards this direction were already mentioned. As a result, the law changed and the UCMAR(s) were established and now the MMAR is a co-responsible entity to address security level 1, level 2 and level 3 and more elaborated plans are now in place.

Ports and port terminals must have their own PSO and PFSO, as established in the ISPS Code. But, in the case of Mexico they were not fulfilling the requirements concerning security incident registers, which should have been created by them concerning the numerous security incidents that were identified, including confiscation of drugs, weapons and hydrocarbons made by the Navy. More importantly, this failure took place despite the fact that these events are classified as high security risks.

14) Asociación Mexicana de Agentes Navieros, represented with the acronym Amanac, in Spanish.
III. Enhancing Maritime Security in Mexico: Privatization, Militarization, or ...

involving confiscation and transportation to official warehouses for future destruction. Kidnapping of port personnel and terminal operators strongly affects port operations and should be handled as security incidents, even when they happen outside the port. Statistics and analysis of maritime security incidents illustrate past actions and shall be open to public scrutiny, ensuring that the government implements barriers to avoid that such events happen again; on the contrary, procedures for how to deal with such incidents in the future are included in the PFSP and must be confidential.

Handling of confiscation of drugs and other restricted items is clearly the duty of the NAUPPRO and customs’ authorities, but it is the duty of the PSO/PFSO to register them accordingly in the respective security incident logs and consider them during the risk evaluation and if needed to amend accordingly the PFSP. The analysis of the root causes of security incidents is the cornerstone of the PFSA, which is the base of the PFSP, but if a new security threat is identified, adjustments are necessary. Therefore it is crucial to keep security incident records updated. Furthermore, all the above-mentioned deficiencies were not detected during the Designated Authority’s audits and inspections and no matter that they went through a second filter, the MMAR, which performed the final revision of the PFSA and PFSP and should require amendments (when necessary) upon their approval. Additionally, authorities of the Tampico Port did not establish a restricted navigation area according to their answer in the questionnaire. A restricted navigation area for the port roadways and within the port proximity area should be established, not only to mitigate security risks, but also for maritime accident prevention.

It is necessary to highlight that it is recommended for the process of recertification of port and terminals to start at least a year before the expiration date of the Declaration of Compliance with the ISPS Code, to avoid that port and terminals continue operating without the required certifications, which could give grounds for suspension of port and terminal operations. Finally, as Kerr (2010) argues, the responsibility for assuring maritime security lies firmly with governments, but private security companies can attend a niche market in support of these official bodies.

Conclusions

Maritime security incidents in Mexico are numerous and involve extraordinary and complex threats such as the plundering of oil platforms, kidnapping and extortion of port personnel and terminal operators and even pirate-type attacks. The government’s security strategy of combining justice reforms and providing more power to the Navy through the formulation of maritime police (NAUPPROs) and UCMARs, as well as including community engagement and the participation of different organisations from the three levels of government is functioning and has improved the overall situation. Mechanisms in place are gradually recovering control of an unacceptable situation, particularly in ports where the military model is being tested. However, this strategy must be followed along with ensuring compliance of the ISPS Code, with the issue of...
record keeping standing out. It is true that the lack of a national maritime security policy has resulted in constant breaches of the ISPS Code provisions and different security procedures at the ports under examination. After twelve years of ISPS implementation, Mexico still does not comply with the requirements of the ISPS Code at an acceptable level, although some improvement is recorded because of the recent security reforms. One pressing need is to introduce a quality system that ensures the proper registration of security incidents: updating these incident records will help in the future improvement of the maritime security framework and the creation of a sustained security culture focused not only on incident prevention, but also on response to and recovery of a major security incident, including resilience plans.

In any case, in order to avoid duality and misunderstanding of security duties due to the recent involvement of the military and the difference in culture, it is recommended to set up a clear division of duties and responsibilities; the establishment of a “no-blame culture” must be considered to ensure the proper registration and thorough analysis of all respective security incidents. It is also recommended to re-evaluate the PFSPs of the ports and all Pemex terminals by considering threats that were not included in the initial creation of those documents; it is also necessary to consider the establishment of a restricted navigation area at the Tampico Port. Last but not least, it is essential to standardise the notion that the process of re-certification shall start in due time (maybe at least a year) before the period of validity of SOC expires to avoid suspension of port and terminal operations. Finally, an extensive study covering the satisfaction level in locations where the militarisation model is already in place (and how this affects trade operations and maritime security) should be performed before its further implementation throughout the country.

References


III. Enhancing Maritime Security in Mexico: Privatization, Militarization, or ...


III. Enhancing Maritime Security in Mexico: Privatization, Militarization, or ...


Mexico's reorganisation of maritime security regime: A new role for the navy and emphasis on energy related infrastructures

Avila-Zuñiga-Nordfjeld, Adriana
Dalaklis, Dimitrios

DOI: 10.1007/978-3-319-74576-3
1 Introduction

Previous research efforts have already pointed out that the current state of implementation and level of compliance with the International Ship and Port Facility Security Code (ISPS Code) in Mexico is rather poor (Nordfjeld and Dalaklis 2016). This chapter will also investigate in a similar direction. It will first provide a summary of the latest reform to Mexico’s national legislation dealing with various important issues of the maritime domain. Then, it will identify the contradictions in the relevant laws, in relation to effective implementation of national legislation and international instruments, with special focus on the ISPS Code. Subsequently, it will study the acceptance of the transferral of the National Maritime Authority from a civil institution (MCT) towards a military one (MMAR) within the four different authorities directly related to the maritime industry’s operations/activities. Finally, findings in relation to field research activities in main Mexican ports and especially important energy hubs are presented, followed by the associated conclusions and recommendations with the aim to improve their security status.

The International Maritime Organization (IMO) communicates via its web site the information that thirty-five (35) different countries located in the American Continent have signed and ratified the International Convention for the Safety of Life at Sea (SOLAS), 1974; Mexico is included in the aforementioned group. The SOLAS 1974 Convention includes Chapter XI-2 concerning special measures to enhance maritime security, and especially Regulation XI-2/3 that enshrines the International Ship and Port Facilities Security Code (ISPS Code). Apart from the ISPS Code, the SOLAS 1974 Convention is used to “operationalize” a very influential safety instrument for shipping operations: the International Management Code.
for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code). Furthermore, in its Chapter XI-1, there are special measures to enhance maritime safety that provide the basis for carrying out inspections of foreign ships in national ports under Port State Control (PSC); the latter can also be described as an exercise of the right of protection of the coastal State, as established in Article 25 of the United Nations Convention on the Law of the Sea (UNCLOS). In the case of Mexico, there is a confusing situation after the country’s last major legal maritime reform, where it was established that the National Maritime Authority shall be executed by the Ministry of Marina (MMAR), and it transferred all Master of Harbours to MMAR; however, the Port Authority remained with the Ministry of Communications and Transport (MCT).

Implementation and compliance with the ISPS Code is a topic studied extensively in the United States and Canada. The US has, indeed, been a pioneer in port security. Already in 1997, 7 years before the ISPS Code entered into force, the US Department of Transportation launched the “Port Security National Planning Guide”, which was “intended to be used by port directors and officers of port security departments in fulfilling their responsibilities toward the development of an effective port security program” (US Department of Transportation 1997). The guide included requirements of a “Security Survey and Risk Assessment” and the development and implementation of a “Security Plan”. Kenneth (2009) pointed out that “the evolution of organized security processes in the maritime sector can be understood as a product of increasing governmental and commercial concerns about the criminal exploitation of seaports, [...] and the rising threat of global terrorism”. In the case of Canada, the ISPS Code has been implemented since it entered into force in July 2004. Rudner (2009) included maritime ports as part of the “Critical National Infrastructure” that must be protected from terrorism and provided emphasis on ports serving the energy sector. The author highlighted the need for “a national strategy/plan for the protection of Canada’s critical national infrastructure against exogenous risks and threats”.

Mexico, similarly to Canada, is one of the largest producers of oil and gas and has a significant number of critical infrastructures, including numerous maritime ports linked to the energy sector. Mexico’s State owned company (Pemex) reported that, as of 1st January 2014, the proven reserves of Mexico’s crude oil were calculated to be 9812 million barrels (MMb), whereas the proven reserves of natural gas were calculated to be 16,549 billion cubic feet (Pemex, Petroleos Mexicanos 2014). This report also mentioned that the biggest volume of proven reserves of crude oil, equivalent to 70%, are located in marine oil fields and only 30% of them are located in terrestrial fields. At the same time, 56% of the proven reserves of natural gas are located in terrestrial fields, with the remaining 44% in marine fields. It must also be highlighted that most of the Mexican ports are directly or indirectly serving the oil energy market for developed marine oil fields.
2 Mexico’s Maritime Reform

To better understand the latest developments in Mexico in relation to the maritime domain, it is important to consider that a few decades ago, the MMAR held the control of ports and the merchant marine; but in 1977 the ex-President José López Portillo reformed the “Law of Public Federal Administration” transferring to the MCT all the activities related to the development of merchant marine, as well as the construction of port infrastructure and the respective administration/operation. However, the MCT and particularly the Harbour Masters (also called Port Captains in Mexico) were never equipped in a satisfactory manner to deliver the functions of maritime safety and security, such as port state control and inspection of vessels. Almost 40 years later, all these functions are (again) reallocated to the authorities of MMAR, with the latest maritime legal reform.

For a rather prolonged period, drug cartels in Mexico were conducting a wide array of illegal activities that resulted in extremely high levels of violence. Considering these implications, as well as less unforeseen crimes such as the theft of hydrocarbons and demands of “extortion payments” to owners and operators of port terminals (Nordfjeld and Dalaklis 2016), the Mexican government attempted the reorganization of its maritime security regime. Not only is efficient use of energy resources important, but “losing” tremendous quantities of oil due to theft is totally unacceptable and must be addressed via the right types of policies. Several existing laws were revised; a new set of regulations was introduced in 2014 that included amendments to the “Law of Ports”, the regulation in relation to the establishment of the “Unified Centre for Port and Maritime Security” (called “UCMAR” thereafter), and the “Law of Navigation and Maritime Trade”, among others. However, the Parliament focused on port security and port installations; it did not include in the regulation the part related to maritime security and the requirements for ships, established in the ISPS Code, such as the Ship Security Officer (SSO), Ship Security Assessment (SSA), the Ship Security Plan (SSP) and the International Ship Security Certificate (ISSC). From April 21st 2014 to June 2017, when the last updates to this chapter were made, there was no institution appointed responsible for maritime security conforming Mexico’s national legislation. Additionally, the creation of the “Military Navy Unit for Port Security/Protection” (“Unidad Naval de Protección Portuaria” and represented with the acronym UNAPROP, in Spanish, called NAUPPRO thereafter) was decided, covering only the part of the ISPS Code related to protection of ports and port installations.

Concerning maritime security, as already mentioned, an important legal instrument is Chapter XI-2 of the Safety of Life at Sea Convention 1974, (SOLAS Convention) which relates to the ISPS Code. This Code is defined by the IMO as “the comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States” (International Maritime Organization 2012). Whereas part A of the Code establishes the mandatory provisions, the non-mandatory (“recommended”) part B provides guidelines about how
to comply with the mandatory requirements of part A. After numerous years of ISPS Code implementation, Mexico does not yet comply with its requirements at an acceptable level, although some improvement is lately recorded, mainly because of the 2014 security reforms (Nordfjeld and Dalaklis 2016).

As highlighted previously, the mandatory Part A of the ISPS Code introduced the obligation for contracting governments to appoint a Designated Authority to carry out certain maritime security duties/responsibilities established in the Code. This Designated Authority holds the responsibility for setting maritime security levels and ensuring compliance with the maritime security measures at all ports (where the ISPS Code applies) through the Port Security Assessment (PSA) and Port Facility Security Assessment (PFSA). The revision, approval and control of compliance of the Port Security Plan (PSP) and Port Facility Security Plan (PFSP), which shall be based upon the PSA and the PFSA, is also included in the respective responsibilities. The development of PSP/PFSP is also related to the activities of the Port Security Officer (PSO) and Port Facility Security Officer (PFSo).

As established by IMO, there are three different security levels: Security Level 1 (normal) requires the minimum protective security measures at all times; Security Level 2, which requires additional protective security measures for the specific period of time that the risk of a security incident is heightened; and Security Level 3, which requires specific protective security measures and may result in the suspension of commercial operations. Security response under Level 3 is transferred to the Government or other organizations responsible for dealing with significant incidents (International Maritime Organization 2012). In Mexico, it is the “Uniﬁed Centre for Port and Maritime Security” (UCMAR) that is responsible for coordination and execution of all security operations under Level 3 and it is the Commander of the Navy Military Zone of each jurisdiction where an UCMAR is established who shall be appointed as the Chairman of that respective UCMAR, as established in provision 8 of Regulation of the UCMAR published on the Ofﬁcial Diary of the Federation, on 21st of April, 2014. This provision also includes the notion that the Harbour Master shall be nominated as the Vice-Chairman of the UCMAR, and, in addition, three employees of each of these institutions shall be selected as advisers. A UCMAR shall be established at each of the 16 Federal Integral Port Administration (s) (FIPAs) designed to receive vessels of over 500 gross tonnage, or which receive vessels sailing international trading routes, according to Provision 6 of the referred regulation.

According to the “Law of Ports” Article 19 SECOND, the UCMAR is a group of inter-institutional coordination between the MMAR and the MCT for the application of and compliance with the ISPS Code. This part was not amended with the Decree. However, since MMAR obtained control of both Master of Harbours and the UCMAR itself, the “inter-institutional character” of this group should be re-evaluated, keeping in mind that MCT will maintain control of the “Fideicomiso de Formación y Capacitación para el Personal de la Marina Mercante Nacional” (represented with the acronym “FIDENA” in Spanish, which may be translated to “Fond of Education and Training of the National Merchant Marine”, and called FETNAMM thereafter). This is the authorized institution for giving the IMO’s
model courses 18.1, 18.2 and 18.3 concerning the ISPS Code, and the only authorized foundation so far, for performing Port Security Assessments (PSA) and Port Facility Security Assessments (PFSA).

Article 19 THIRD, paragraph II of this law highlights that “the UCMAR shall apply all the dispositions and response measures within the framework of the Chapter XI-2 of the SOLAS 1974 Convention, comprising the ISPS Code and ensure the establishment of a series of functions and actions for each of the respective three security levels”. This is part of the maritime security reforms that took effect on the 21st of April 2014. However, because of lack of knowledge about the reform itself, the MMAR did not fully exercise its authority and the Harbour Master was erroneously recognized as the authority (for the ISPS Code) by the PFSOs and port agencies. The UCMAR is responsible for the revision of PSA/PFSA, which covers the security risks evaluation for ports or port facilities, which shall be the base for developing the PSP/PFSP, submitted and approved by the Designated Authority. The responsible person for developing the PSA/PFSA and PSP/PFSP is the Port Security Officer (PSO) or Port Facility Security Officer (PFSO), including compliance with all requirements established in the ISPS Code and reflected in the PSP/PFSP as training, exercises, practices, inspections audits and modifications via formalised procedures to the plan.

In another research of Nordfeld and Dalaklis (2017), it was rightly pointed out that the PSO/PFSO must attend security incidents and keep incident security records updated, which must be considered in the risk evaluation and integrated into the security plan to achieve a constant reduction of risks and continuous improvement of port and maritime security. UCMAR shall verify, among other aspects, that security incidents are properly recorded in the security incidents register; even with MCT supervising the port authority, the UCMAR is responsible for control of compliance with the ISPS Code and co-responsible for the revision and approval of PSA/PFSA and PSP/PFSP, according to its Regulation, Article 7, paragraph II, which states that: “[UCMAR] shall participate in the evaluation of risks of maritime and port security, previous to the elaboration of the security plans and it shall propose the necessary modifications and updating to those plans”. Paragraph III of this article, mentions that once the plan has been approved, the UCMAR shall participate in the verification and control of compliance with plans, ensuring their effective implementation. Findings of the above mentioned study included inconsistencies within the data of the necessary security incident records, or even their total absence. Neither the MMAR nor the MCT has effectively addressed the issue of security incident record keeping.

The UCMAR is currently performing the responsibilities of a Port Security Committee, a committee recommended by the ISPS Code to coordinate security procedures and measures. Under the UCMAR, there is also the Port Security Assessor Committee, which is normally integrated by the UCMAR and customs-immigration authorities operating at the port; the management of the port operator and port terminals is also included. Additionally, municipal and regional Governments with associated interests in that jurisdiction are part of the committee. However, it is important to consider the need to balance the openness of an advisory
committee with the need to protect the confidentiality of sensitive security information (International Maritime Organization 2012).

In 2016, the President of Mexico, Enrique Peña Nieto, presented a law initiative to amend and improve diverse provisions of the “Law of Public Administration”, “Law of Navigation and Maritime Trade” and the “Law of Ports”. The aim was to transfer the control, inspection, vigilance and other activities related to the merchant marine and the maritime industry, including Harbour Masters from a civil authority (MCT) to a military one (MMAR). However, a significant exclusion was port development and administration apparatus, including the port authority, which was previously exercised through Harbour Masters. This law initiative was approved by the National Congress without any change and published as a Decree on the Official Diary of the Federation (ODF) on the 19th of December 2016.

This legal document establishes the new attributions of the Ministry of Marine, which entered into force on the 17th of June, 2017. Every authorized port shall have a Master of Harbour, which will be administrated by MMAR with a delimited maritime territorial jurisdiction, which, according to Article 9 of the decree, shall have attributions to authorize bear away and bear off as well as customs clearance of naval craft; flag and register Mexican vessels and naval artefacts; grant permissions for offering maritime passenger transport services and nautical tourism within the waters of jurisdiction; regulate and monitor that the nautical routes meet the required conditions for safety, depth, marine signs, maritime traffic control and nautical assistance; and inspect vessels, among others.

The duties and responsibilities of the NAUPPRO should also be (re-)evaluated and confirmed. This unit currently has the functions of a coast guard. It is under the control of the Commander of the Navy Zone at each port, who is the President of the UCMAR. However, its guidelines concerning duties and responsibilities are not clear enough with respect to its duties under the UCMAR. Yet, these units have the responsibility of port protection under the control of the Commander of the Navy Zone, and they must ensure control and compliance with ISPS Code requirements at the port and give all necessary information to the Commander, who holds the role of Chairman of the UCMAR, may inform the rest of this group of actions taken by the NAUPPRO. The actual Guidelines of NAUPPRO are currently too general and rather vague. Due to their military discipline, they do not take actions to ensure compliance with ISPS Code requirements if they do not receive concrete and specific orders or if it is not clearly established and requested in their procedures. The development of rules/protocols with specific and concrete duties for this unit is recommended. Security duties performed by the NAUPPRO may include, among others, considering that currently they only attend the ISPS Code section related to port installations:

- Control/verification that all maritime ports and terminals are operating with an updated Statement of Compliance (SOC).
- Revision and control that all ports and terminals have employed a certified PSO/PFSO with an updated and valid certificate.
• Revision and control that all personnel from ports and terminals with security duties have been certified with the necessary training concerning the required course 18.2 as established in the ISPS Code.

• Revision and control that all personnel from ports and terminals without specific security duties have been certified with the necessary training concerning the required course 18.3 as established in the ISPS Code.

• Develop and keep the official register of maritime security incidents for that specific port.

• Revise and control that all PSO/PFSO keep their own registers updated for reporting maritime security incidents.

• Participate in the revision and analysis of Port Security Assessments (PSA) and Port Facility Security Assessments (PFSA), for terminals.

• Participate in the inspections for approval of PSA/PFSA.

• Participate in the revision and analysis of Port Security Plans (PSP) and Port Facility Security Plans (PFSP) and make observations for necessary modifications to those plans.

• Participate in inspections and audits for approval of PSP/PFSP before the issuance of the Statement of Compliance (SOC).

• Carry out random inspections on scene and general inspections to verify the compliance of PSP/PFSP.

• Plan, coordinate and carry out security drills (level 3) at a minimum interval of once a year with no more than 18 months between them.

• Participate in the evaluation of security drills (level 3).

• Participate in and make the necessary observation for the external security audit, which shall be performed with a minimum interval of once a year.

• Develop and keep updated the register of approved PSA/PFSA; PSP/PFSP; drills; inspections and other relevant operations for availability to IMO, in the case of mandatory audits.

Agreement number 039 for the creation and activation of 19 NAUPPROs at the main maritime ports of Mexico was published on the 31st of March, 2014, on the Official Diary of the Federation. However, only 14 in total have been created and activated up to this point. The activation of NAUPPROs at the ports of La Paz, Puerto Vallarta, Puerto Chiapas, Matamoros and Dos Bocas is still lacking; at this last port, the official creation of the UCMAR is also lacking.

The Presidential Decree recently reformed the country’s legal framework and allowed the complete shift not only of maritime security, but also of the safety aspect (including the port-state control function) from a civil authority (MCT), to a military one (MMAR). The previous failures of the Mexican Designated Authority are associated with a large number of security incidents and various accidents which, through poor inspections, have contributed not only to loss of property at sea, but also to human casualties and significant marine pollution. Aranda (2016) pointed out that while the Chamber of Senators analysed the initiative of law, three maritime accidents that occurred that summer can be used as evidence of deficiencies in the system under MCT. The Harbour Master of Tampico Port has also been denounced...
for corruption and abuse against fishermen. More specifically, MCT employees were accused of corruption by the owners of the fishing vessels “Rastreador”, “Banpesca”, “Fenicio”, “Astur” and “Tampico Star”. All these argued that they were forced to hand over a shrimp carriage quota to personnel from that institution, to be able to work (Vergara 2016).

The initiative emphasized the convenience of defining one National Maritime Authority to comply with national and international obligations and the need to delimitate and redistribute the attributions that are exercised by both institutions, the MMAR and MCT. However, several duties and responsibilities are still “shared”. While the MMAR is responsible for implementation and compliance with the ISPS Code, the MCT holds the port authority role and is responsible for imposition of sanctions related to violations of the Code. On the positive side, the new legal regime emphasises that MMAR currently has the human and material resources necessary to comply with the exercise of the national sovereignty and authority in the Mexican marine zones, as well as to guarantee the compliance of the port with the national (maritime) legal framework.

In summary, the reforms to Article 8 SECOND of the referred “Law of Navigation and Maritime Trade” established the new attributions of the Ministry of Marine, and empowered MMAR to approve licenses for passenger and tourism maritime transport services with small boats, authorize vessels to bear away and bear off as well as customs clearance. Flag and registration issues of vessels, administration of the national registers of maritime crews and ships, as well as inspection and verification of national and foreign vessels are included in those tasks. Additionally, compliance with international conventions as well as national legislation and official Mexican norms related to maritime safety and security is another of its tasks.

At the same time, the Decree reformed Article 8 of the “Law of Navigation and Maritime Trade”, concerning the new attributions of the MCT, confirmed that MCT will continue to lead the administration of ports, as well as the training framework of the merchant marine. A significant inconsistency is that the decree modifies Article 7 of the “Law of Navigation and Maritime Trade” and establishes that the “National Maritime Authority” is exercised by the Federal Executive Power through MMAR for the exercise of national sovereignty, dealing with maritime safety and security issues, as well as exercising the Right of the State to be applied at the Mexican marine zones, while Article 9 B establishes that MCT will exercise its functions at the ports through the Offices of Services to the Merchant Marine. Additionally, the “Law of Ports”, Article 16, clearly establishes that the Port Authority is exercised by the Federal Executive Power through MCT, which will be exercised through the “Offices of Services to the Merchant Marine” established at all ports.

Vessel inspections are currently performed at the dock in the ports of Mexico, while according to common practice this should be done outside in the open ocean between 12 and 24 miles, in the contiguous zone. MMAR should evaluate the allocation to Harbour Masters of a certain number of the interceptor-patrols they already have or assess the acquisition of some Ocean Patrol Vessel(s) Defender II, which is a relatively small naval vessel designed to perform coastal defence duties, but large and seaworthy enough to patrol offshore areas in the open ocean.
Concerning the offshore area of Campeche, the control centre for maritime traffic was formerly managed and operated by Pemex, a private company. To ensure the proper exercise of the maritime authority in this area, MMAR should recover the control and operation of this centre.

3 Research Methodology of Field Activities

The research methodology of the current study includes semi-structured interviews with Harbours Masters, Directors of Customs Maritime Units, Directors of ports, PFSOs from ports and certain number of hydrocarbons terminals, Presidents of UCMAR (1st Commander of the Navy Zone, Navy Sector or Navy Station) and Commandants of the port and maritime police (Naval Unit for Port Security, also called NAUPS) and the Gulf’s Navy Force. Additionally, participant observation at the terminals and Harbours Master’s installations and ports, including not only the land areas but also the maritime passages took place; visits were made on board oceanic patrols of the Mexican Navy. The visits to the mentioned ports in Mexico had an average duration of a week at each port.

The pool of data included the leaders of the mentioned institutions from the ports of Altamira and Tampico (Tamps.), Tuxpan, Veracruz and Coatzacoalcos (Ver.), Dos Bocas (Tab.), Ciudad del Carmen (Campeche), and Progresso (Yuc.) as well as another Hub Port from the Pacific in Mexico. By doing this, the researcher covered the four pillars for the operation of the port. The pool of data is deemed sufficient, based on the fact that it includes eight out of sixteen FIPAs in Mexico where the ISPS Code applies, representing 50% of them and seven out of seven (100%) FIPAs situated in the Gulf of Mexico, where oil exploration and production activities take place. One State-Owned Integrated Port Administration (Ciudad del Carmen, Campeche) where most of the oil activity is concentrated was also included in the study. Two loose interviews with top directors from MMAR were performed on key themes identified from issues prevalent in the analysis of the interviews with Presidents of the UCMAR and Federal FIPAs. From the total number of persons invited to participate, representing Master of Harbour offices at these nine cited ports, only one of them rejected the invitation. The same figures correspond to representatives from the maritime customs units (one) and directors from FIPAs (one) as well as the PFSO from that same port, who due to extreme work volume had to decline the interview.

The purpose of the study was described to the participants via an information cover-sheet letter where the research objectives were explained, clarifying that their participation was voluntary, confidential and without any economic contribution, or gifts. The Research Ethics Committee of the World Maritime University approved the study. The total of interviewed participants was 57 persons, all of whom worked in areas of maritime safety and security. Interviews were carried out in the participants’ workplaces by the researcher, tape recorded and transcribed verbatim. Data was examined line-by-line, and the main categories and themes were identified and
coded using thematic analysis and constant comparison of data. The researcher searched thoroughly for all divergent views to form a rich description of different factors.

4 Results

From the interviewed subjects with functions of Master of Harbour, 75% expressed their approval to be transferred to the MMAR and supported the law decree, while 25% strongly disapproved of the transfer between the institutions. An important conclusion is that the people interviewed were either very much in favour or very much against the change. 87.5% of Directors of maritime customs units and 75% of Directors of FIPAs supported the law decree; at the same time, 100% of Presidents of UCMAR held a positive view. The same figures correspond to Commandants from the NAUPPRO (coast guard-navy), whereas 87.5% of Port Security Officers (PSO) supported the transfer of Master of Harbours to MMAR; and 80% of the interviewed subjects functioning as Port Facility Security Officers (PFSO) from hydrocarbon terminals supported the transfer.

Twelve categories were identified that either prevent or promote the transfer of Harbours Master from MCT to MMAR: (I) poor performance of Harbours Masters from the MCT; (II) acute lack of human and material resources available for Harbours Masters to comply with their duties and responsibilities in a satisfactory manner; (III) high exposure to corruption on the part of Harbours Masters related to Mexican crime ring organizations due to death threats against them or their families; (IV) fear on the part of Harbours Master of losing their jobs in a late stage of their productive life; (V) uncertainty on the part of Masters of Harbours with respect to their salary level, working rights and pension schemes; (VI) improvement of salary and working rights for Masters of Harbours and their personnel with the transferral to MMAR; (VII) already high participation of the Mexican Navy performing duties that correspond to Harbour Masters; (VIII) fear on the part of directors of port administrations of lack of knowledge, stubbornness and unwillingness/inflexibility to negotiate on factors related to business issues with respect to authorities from the Mexican Navy; (IX) security improvement for offshore installations and vessels serving the oil market; (X) trust in a significant improvement of maritime safety and security on the part of directors of maritime customs units with the transfer of Harbour Master offices to the Ministry of Marine; (XI) bigger and better capabilities to combat crime ring organizations that are using port installations for transport of drugs, weapons, money laundering and transport of stolen hydrocarbons, and finally; (XII) need to provide juridical support and attributions to the MMAR for activities already performed by the Navy and which are currently outside their juridical attributions.
5 General Discussion

A number of participants’ quotes are used to better illustrate the associated data. Concerning category (I) poor performance of Masters of Harbours, one of the quotes that best illustrates the situation is taken from participant number 6 who said: “unfortunately, the master of harbours have lost a lot of authority and it is very sad that nobody takes them seriously anymore”. This situation might be explained with category (II) acute lack of human and material resources available for Harbour Masters to comply with their duties and responsibilities in a satisfactory manner. The statement that best explains this aspect is from participant 1-G, who claimed that: “the Maritime Designated Authority somehow is suffering a separation of attributions and material resources, because since 1940 the Mexican Navy; [...] used to give all the required support to Harbours Masters [...] but when they were transferred to MCT, [...] all the naval craft and necessary equipment was left with MMAR, including navy vessels, ocean patrols, boats for search and rescue operations and helicopters. Then, with these limitations the MCT started to function since 1976 and until today”. Interestingly enough, 100% of the participants pointed out the acute lack of resources for Harbour Masters to carry out their duties in an adequate manner.

Another reason for the loss of authority of Harbour Masters, can be explained with category (III) high exposure to corruption on the part of Harbour Masters related to Mexican crime ring organizations due to death threats against them or their families; as the case of participant 36 who affirmed “I have one year and seven months that I am working under death threats. Constant threats by phone [...] I have moved my home and my family out of the city. There is no other way. And what can I do? I have the need to work. But tell me, where is not the same”?

Participants highlighted the already high participation of the Mexican Navy performing duties that correspond to Harbour Masters (category VII). Yet, several directors of ports manifested their fear of lack of knowledge and inflexibility to negotiate on factors related to business issues with the Mexican Navy (category VIII). To illustrate this aspect, one of them (26) is quoted: “I believe that the marina has given courses to their people but I do not think that they have much experience and knowledge concerning the operation and administration of merchant marine”. This was a view was shared by a few Harbour Masters. One of them (18) affirmed: “[...] one of our functions [...] is the fluidity of the port. They are accustomed to command, and to apply correctness regardless of the problem, here everything is about flexibility and judgment. They do not have it”. On the other hand, 75 per cent of as FIPAs’ directors were very positive about the transferral. To illustrate their attitude, respondent 49 quoted: “[...] I believe that the objective of this project is to strengthen the Harbour Master to be able to do their duties in an efficient and effective way concerning vigilance and control of ports.”

Category number (X) envisions a significant improvement of maritime safety and security on the part of directors of maritime customs units with the transfer of Harbour Masters offices to MMAR; this can be explained with a quote from
participant 6: “I have had the opportunity to work in the ports where the control of the Harbour Master was already been taken by the Ministry of Marina and it has been immensely positive. There was a huge leak of information that could only be controlled with the interference of the Navy. It has been very good. [...] I am waiting for them to do so, here too”. In the agreement between MMAR and the MCT (2009), it is stated that the financial and operative capacity of crime ring organizations has allowed them to access strictly confidential information. Therefore, it is important that MMAR implement an anti-corruption programme for the transfer of MCT employees to Marina to stop old corruption and leaking of information practices.

A statement from respondent number 36 reflects category (XI): bigger and better capabilities to “fight” crime ring organizations using port installations for criminal activities: “the infrastructure to properly exercise the maritime authority is in MMAR through the Navy. The international conventions originally signed by the MCT are already taken by the MMAR, why? It may be because we do not have the equipment and human resources that they have”.

6 Conclusion and Recommendations

It is a rather self-explanatory fact that the Presidential Decree under discussion has significantly influenced the Mexican legal maritime framework; it allowed the shift of maritime safety and securities responsibility, from a civil authority (Ministry of Communications and Transport, MCT) to a military one (Ministry of Marine, MMAR). The very high level of acceptance between the four pillar institutions involved in maritime safety and security operations (both at port and at sea) such as Maritime Customs Units, Military Navy Zone-with its respective UCMAR, Federal Integrated Port Administrations, maritime police-represented by the Navy Unit for Port Protection (NAUPPRO), and finally the Harbour Masters themselves is a very strong indicator.

However, Mexico has to significantly improve the current level of performance; even if the change of the designated authority may contribute to the achievement of this goal, the MMAR must ensure the application of integrity and anti-corruption programs during the transferral process, to disconnect from the main causes of past failures. Further reforms to the Law of Navigation and Maritime Trade, Law of Ports and the regulation of the UCMAR shall be enacted with regard to appointing the institution responsible for implementation and compliance with the ISPS Code, with respect to maritime security, in relation to the security requirements for the operation of vessels. The transfer of the Port Authority from MCT to MMAR should be evaluated to avoid triangulation of the activities related to the maritime authority, such as imposition of sanctions. Most FIPAs are under the control of MCT and the simultaneous execution of both roles (acting as the performer and evaluator) should be avoided.
Strengthening the maritime security regime and especially its interface with energy resources remains an action of priority in order to “avoid unnecessary casualties” as a result of illicit activities and theft. Similarly, in order to enhance the level of maritime domain awareness (MDA) in Mexico, as well as introduce a forward way of thinking about conducting maritime security operations, the MMAR could also recover control of maritime traffic centres (which are currently operated and administrated by Pemex, including the offshore and oil production area of Campeche). Better information is a prerequisite for the optimal allocation of resources. The allocation of offshore patrol vessels or “Deterrence” patrols, as well as the required personnel to operate them at the disposal of Master of Harbours could allow the latter to perform vessel inspections at the contiguity zone if they consider so necessary. Additionally, tailor made training will also be needed to build the necessary human capacity and expertise that it is not yet available; the introduction of a “no-blame” culture could also be considered. Finally, MMAR must also avoid misuse of high security trained resources in duties that are outside their competence and especially avoid allocating to the maritime police (NAUPPRO), duties and responsibilities that must be performed by staff belonging to Harbour Masters.

References


Further Reading


Integrating the procedures of reporting port security incidents and the follow-up investigation to build a national maritime security policy: A case study in Mexico.

Avila-Zuñiga-Nordfjeld, Adriana
Dalaklis, Dimitrios

WMU Journal of Maritime Affairs
https://doi.org/10.1007/s13437-018-0154-3. (online version)
Integrating the procedures of reporting port security incidents and the follow-up investigation to build a national maritime security policy: a case study in Mexico

A. Ávila-Zúñiga-Nordfjeld\textsuperscript{1} \& D. Dalaklis\textsuperscript{2}

Received: 23 April 2018 / Accepted: 24 August 2018/Published online: 20 September 2018
© World Maritime University 2018

Abstract
This paper aims to improve port security measures in developing countries via integrating the procedures of incident reporting and the associated follow-up investigation, hinging on the Mexican experience. The analysis examined port security at Mexican ports, where stakeholders were interviewed on the subject to identify the challenges and opportunities for security incident reporting, updating of security incident records and facilitation of the follow-up investigation. Then, a qualitative security model was developed; under this new framework, incident reporting, incident investigation, the re-assessment of security threats through the Port Facility Security Assessment (PFSA) and the necessary modifications to the Port Facility Security Plans (PFSP) were all integrated. These subjects were all incorporated into a “transparent port security incident reporting tool”. This tool was implemented at all ports in Mexico, where the International Ship and Port Facility Security Code (ISPS Code) applies, by the National Maritime Authority. This demonstrated in a real case through “action research”, the improvement of port security framework in the country. Measurements were executed every quarter throughout the year 2017 and the incident-reporting instrument was adjusted accordingly. The results demonstrated a significant improvement in reporting security incidents, with the increase from absolutely nothing (zero) to 57 providing a strong indicator of success. In addition, 56% of those reported maritime incidents were also associated with recommendations to be integrated into the PFSA and respective PFSP. Collecting accurate and immediate information/evidence material while reporting security incidents is crucial for effective incident investigation and continuous improvement of the PFSP.

\textsuperscript{1} Maritime Administration: Law, Policy, Safety and Security, World Maritime University (WMU), Malmö, Sweden
\textsuperscript{2} Safety & Security, World Maritime University (WMU), Malmö, Sweden
1 Introduction

Concerning port (and maritime security), one of the most important instruments of international law is the set of maritime security regulations developed by the International Maritime Organization (IMO) that are formulating the International Ship and Port Facility Security Code (ISPS Code); the ISPS Code is “the comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States” (International Maritime Organization 2012). Whereas Part A of the Code establishes the mandatory provisions, the non-mandatory (“recommended”) Part B comprises guidelines about how to comply with the mandatory requirements of Part A (International Maritime Organization 2017). In any case, core instruments of the ISPS Code are security incident reports and security incident investigation.

The ISPS Code Part A establishes in section 17 that a Port Facility Security Officer (PFSO) shall be designated for each port facility. Section 17.2 establishes the duties and responsibilities of the PFSO; from these, it is noteworthy that according to paragraph 8, this person is involved with “reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility.” Therefore, it is the responsibility of the Port Security Officer (PSO) or Port Facility Security Officer (PFSO) to deal with security incident reporting and keep the associated records updated. Furthermore, security incidents must be considered in the evaluation of risk for the Port Security Assessment (PSA) or Port Facility Security Assessment (PFSA) and integrated into the Port Security Plan (PSP) or Port Facility Security Plan (PFSP) to constantly reduce risks and continuously improve port (and maritime) security. Ávila-Zañiga-Nordfjeld and Dalaklis (2017a) have already pointed out that “the analysis of security incidents’ root causes is the cornerstone of the PFSA, which is the base of the PFSP; but, if a new security threat is identified, adjustments are necessary. Therefore, it is crucial to keep security incident records updated.”

In addition, it must be well documented within the respective PFSP the procedures for reporting security incidents. Port facility security incidents are normally divided into two categories: (1) those considered sufficiently serious/grave that the PFSO/PSO must report to relevant authorities for their official investigation. These include, but are not limited to, unauthorized access to restricted areas within the port facility; unauthorized carriage or discovery of drugs, weapons, or prohibited items within the port facility (including those found in ships’ carriage); incidents for which the media is aware; bomb warnings and unauthorized disclosure of the PFSPs, among others; (2) those security incidents of less serious nature. These events require updating of the security records, but they might be investigated directly by the PFSO/PSO to discover the causes and take the corresponding actions to implement measures in order to avoid their repetition in the future. These may include breaches of screening points, inappropriate uses of passes or terminal identification cards, suspicious behavior in or near the port facility, and unsecured access points (International Maritime Organization 2012). In any case, security threats, breaches of security, and security incidents, including date, time, location, response to them, and the person-authorities to whom they were reported,
must be recorded and documented in the security incidents records. In certain countries, the maritime designated authorities have specified the type of maritime and port security incidents that must be immediately reported to them for official investigation. Indicative examples include terror attacks; bomb warnings; hijack, armed robbery against a ship; discovery of firearms, drugs, weapons, and explosives; and unauthorized access to port facilities and restricted areas (International Maritime Organization 2012).

After almost 14 years from the ISPS Code’s implementation, Mexico does not comply yet with its requirements at an acceptable level. On the positive side, some improvement is recently recorded because of the maritime reforms of 2014 and the latest maritime and port reform of December 2016, when the National Maritime Authority was transferred from the Secretariat of Communications and Transport (SCT) to the Secretariat of the Navy\(^1\) and called SEMAR hereinafter (Avila-Zúñiga-Nordfeld and Dalaklis 2017a). Avila-Zúñiga-Nordfeld and Dalaklis (2017b) explained that in Mexico, it is the Centro Unificado Para La Protección Marítima Y Portuaria (CUMAR),\(^2\) which is responsible for the port and maritime security. According to the Law of Ports Article 19 SECOND, the CUMAR is a group of inter-institutional coordination between the SEMAR and the SCT for the application of maritime security measures; effective prevention and/or dealing with maritime and port security incidents is the primary aim (Cámara de Diputados del H. Congreso de la Unión, México 2017a). Article 19 THIRD, II paragraph establishes that the CUMAR shall apply all the dispositions and response measures within the framework of the Chapter XI-2 of the SOLAS 1974 Convention, comprising the ISPS Code. According to its Regulation, provision 6: “a CUMAR shall be established at all the 16 ports (FIPA\(^3\)’s, where the Code applies.” Additionally, provision 8 of this regulation establishes that it is the Commander of the Navy Military Zone of each jurisdiction, where a CUMAR is established, who shall be the President of that respective CUMAR (Cámara de Diputados del H. Congreso de la Unión, México 2017a).

Additionally, serious maritime incidents must be officially investigated as required by the Code of the International Standards and Recommended Practices for a Safety Investigation into a Marine Casualty or Marine Incident (the Casualty Investigation Code—CI Code). The CI Code was adopted by IMO on 16 May 2008 through resolution MSC.255(84), establishing diverse provisions in Chapter XI of the SOLAS Convention, making several parts of the Code mandatory (International Maritime Organization 2008). The Code establishes the State obligations, responsibilities, and different techniques of casualty and incident investigation. Concerning the State obligations, it must be highlighted that IMO Resolution A.1070 (28) imposes an obligation on Flag States to implement mandatory instruments (IMO 2013). In the case of Mexico, the CI Code was adopted and published in the Official Diary of the Federation on 21 November 2013 (Código de Normas Internacionales y Prácticas Recomendadas para la Investigación de los Aspectos de Seguridad de Siniestros y Sucesos Marítimos–Código de Investigación de Siniestros, in Spanish). Though the CI Code mainly focuses on safety issues, it also addresses maritime security incidents in Chapter 19, which deals with “acts of unlawful interference.” In such cases, authorities responsible for ISPS’s compliance must be involved. Provision 19.1 of the CI Code states: “If in the course of a marine safety investigation it becomes known or is

\(^{1}\) Secretaría de Marina, in Spanish and represented with the acronym SEMAR.

\(^{2}\) Unified Centre for Port and Maritime Security in English, and referred to as CUMAR thereafter.

\(^{3}\) Federal Integrated Port Administration
suspected that an offence is committed under articles 3, 3bis, 3ter or 3quarter of the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988, the marine safety investigation Authority should immediately seek to ensure that the maritime security Authorities of the State(s) concerned are informed.”

The safety or security official investigation in relation to a marine casualty or a port and maritime incident, respectively, must run in parallel to the judicial investigation. The objective of such investigation, following the purpose of the CI Code, is not to deal with apportionment of blame or liability, but to learn the lesson and understand the causal factors of why a particular incident occurred. Another objective is to prevent similar accidents/incidents from reoccurring, via reporting them to IMO (in the case of serious marine accidents is essential and mandatory), so that the entire maritime community can learn of the specific event and avoid similar mistakes in the future. Of significant importance is also the fact that in the case of very serious maritime security incidents, there must be a reassessment of the PFSA/SSA and adjustment of the PFSP/SSP, accordingly, as required by the ISPS Code. Part II of the CI Code comprising chapters 4-14 contains mandatory provisions, while Part III including chapters 15 to 26 contains recommended practices regarding maritime accident and incident investigation. Chapter 6 provides the obligation for Coastal and Flag states to conduct a marine safety investigation into every very serious marine casualty/incident; with the understanding that every incident that results in “significant loss of life, severe damage or pollution with significant political implications” is considered as a very serious one and, therefore, it must be officially investigated (IMO 2014).

Even though the official security incident investigation is not judicial (it runs parallel to the judicial), official maritime and port security investigators from the Maritime National Authority have the burden of proof. This means that they have the obligation to prove their conclusions reached in an incident investigation, which must follow the basic principles of natural justice and procedural fairness, as well as present evidence if required. The Maritime Authority shall also ensure that other relevant authorities and interested parties as terminal operators, ship owners, Flag Administration, P&I clubs and other port and terminal insurance’s representatives, classification societies, salvage organizations and lawyers representing cargo owners, crew members are properly notified and that they are given instructions about how to handle of evidence material. The ship’s master, crew, and personnel shall also be reminded about the prohibition of removal of evidence and their right in respect of legal representation for interviews/testimonies, as well as their right to be protected against self-incrimination, also for the official maritime incident security investigation.

It is common that after a maritime incident, both the maritime security investigation body and the judicial authorities attend the event simultaneously to investigate the incident and collect evidence. In most cases, in the absence of specific legislation to the contrary, the judicial body would have priority and would immediately start to conduct interviews and collect testimonies for a possible prosecution. This deviates from the principles of incident security investigation and, therefore, it is important that incident security investigators conduct a separate analysis not directly based on the judicial proceedings. This, of course with the override understanding that cooperation between authorities will allow to conduct both judicial and security incident investigations in parallel, as IMO (2014) points out by referring to the CI Code, chapter 9. Furthermore, Chapter 21 of that Code, provision 21.2 establishes the obligations for the marine safety investigating State(s), which shall ensure the implementation of an appropriate framework within the State for, among other aspects:
1. The designation of investigators to the marine safety investigation including an investigator to lead the marine safety investigation;
2. The provision of a reasonable level of support to members of the marine safety investigation from other authorities;
3. The development of a strategy for the marine safety investigation in liaison with other substantially interested States.

These three aspects of Provision 21.2 of the CI Code concerning the obligation of the State should also apply for port (and maritime) security incidents. The maritime security investigation State should also provide every effort to facilitate the maritime or port security investigation in order to improve maritime security at its own ports and territorial sea and to protect its own national interests.

As mentioned before, in the case of Mexico, the institution responsible for the implementation and compliance with the ISPS Code is the CUMAR; this institution is also responsible for revision and approval of PFSA/PSA and PFSP/PSP (as well as the Ship Security Assessment-SSA and Ship Security Plan-SSP for vessels bearing the national Flag). Therefore, the CUMAR is also liable to investigate serious maritime and port security incidents and ensure the re-assessment of PFSA/PSA and PFSP/PSP, SSA/SSP (of national Flag) after a serious maritime or port security incident. The CUMAR representatives are the first authority notified on a security incident and the first to arrive at the place of the event. They should continue to cooperate with the judicial authorities for the judicial investigation. In parallel, but separately, they shall perform their own maritime or port security investigation of that particular event, according to the principles of the CI and ISPS Code. Finally, they should provide recommendations to PFSO/PSO (or Ship Security Officer-SSO) about how to prevent such events from reoccurring and ensure that these Officers include those threats into the PFSA/SSA and that PFSP/PSP/SSP are amended accordingly.

Recalling that there is a growing concern about maritime and port infrastructure as targets of a terror attack, as well as factoring in the importance to keep high maritime and port terminal security standards, investigation procedures of security incidents were studied, along with the way of reporting those port security incidents. The issue was examined from the unique perspective of Mexico’s coastlines and associated port infrastructure and at the same time addressing the demands placed on the CUMAR by international and national legislation. To facilitate this, a Model for Port and Maritime Security Incident Investigation was developed. On the bases of this Model, a new and “transparent incident-reporting tool” was created, building the bridge between PFSA, PFSP, and port security incident investigation, as illustrated in the paragraphs that follow. Due to its lengthy extent, the transparent incident-reporting tool is presented in full detail as Annex I in the English version and within Annex II in the Spanish one. Additionally, the crossovers of the respective research areas are depicted in Fig. 1.

2 Research objectives

The first objective of this paper is to study the current situation of port security in Mexico, with particular focus on the compliance of security assessments, security
plans, incident reporting, and incident investigation to develop an analytical transparent incident-reporting tool that integrates all the procedures of these ISPS Code requirements.

The aim is that this instrument supports security incident reporting and improves PFSA, its respective PFSP and port/maritime security incident investigation. Acquiring all relevant information of a particular incident in this instrument will facilitate to learn the lesson from that event and use it for updating of PFSA and respective Security Plans. It would also provide all necessary information to official investigators to follow-up the event and instruct the implementation of measures to prevent its re-occurrence.

The second objective of this paper is to examine port security at Mexican ports from an incident reporting and investigation perspective, by implementing this instrument at all ports in Mexico where the ISPS Code applies. This, with the support of the National Maritime Authority, demonstrating in a real case through “action research,” the contributions of this instrument to improve incident reporting, incident investigation, PFSA and PFSP.

The third objective of this paper is to demonstrate the use of this tool for a multilevel analysis of port security threats to identify the problem areas and contribute to set up the strategies for the development of a national maritime security policy.

### 3 Research methodology

The research methodology includes semi-structured interviews conducted to Master of Harbors, Directors of Customs Maritime Units; Directors of ports; PFSOs from ports and certain terminals that are dealing with hydrocarbons; Presidents of CUMAR (1st Commander of the Navy Zone, Navy Sector or Navy Station); Commandants of the Unidad Naval de Protección Portuaria and called hereinafter UNAPROP. At the same

---

4 Naval Unit for Port Security.
time, participant observations at Maritime Customs Units, Master of Harbors installations, ports, and port terminals—including not only the land areas, but also the related maritime passages—were conducted; all these were visited on board patrol vessels that were made available by the Mexican Navy. The visit to the mentioned ports in Mexico was conducted from the 10th of October 2016 to the 9th of December 2016, with an average of a week devoted to each port. Another 6-day visit to one of the three largest ports of Mexico in the Pacific area was conducted in April 2016, where semi-structured interviews and participant observation were performed. The poll of data included the leaders of the mentioned institutions from the ports of Altamira and Tampico (Tamps.), Tuxpan, Veracruz and Coatzacoalcos (Ver.), Dos Bocas (Tab.), Ciudad del Carmen (Campeche), and Progresso (Yuc.), as well as another hub port from the Pacific in Mexico. By doing this, the four pillars for the operation of ports were covered. The pool of data is deemed sufficient, based on the fact that it includes eight out of 16 FIPA in Mexico where the ISPS Code applies, representing a coverage of 50% of them and seven out of seven FIPAs situated in the Gulf of Mexico, where oil exploration and production activities take place, achieving a 100% coverage of them. One State-Owned Integrated Port Administration (Ciudad del Carmen, Campeche) where most of the oil activity is concentrated was also included in the study.

From the persons invited to participate and representing Master of Harbor offices at these nine ports, only one of them rejected the invitation. The same figures correspond to representatives from the maritime customs units (one) and directors from FIPAs (one), as well as the PFSO from that same port that due to extreme work volume had to decline the interview. Qualitative semi-structured interviews were used to allow new viewpoints to emerge freely, particularly about opinions and perceptions concerning the participants. This method is valuable to study opinions and fears of people when changing processes and systems, especially after the shift of maritime safety and security responsibility, as well as port state control from SCT to SEMAR. The purpose of the study was described to participants in an information cover-sheet letter where the research objectives were clearly described, explaining that their participation was voluntary, confidential, and without any economic contribution or gifts. The total number of interviewed participants was 57 persons, all of them practicing in areas of maritime safety and security, or customs units. Interviews were carried out in the participant’s workplaces via taped recorded and transcribed verbatim. Data was examined line-by-line, and the main categories and themes were identified and coded using thematic analysis and constant comparison of data.

At that stage of the research and after the establishment of 15 different themes, “Action Research” was integrated into the methodology with the aim to improve the level of maritime security in the country under examination. Action research is a form of interactive inquiry process that balances problem solving; actions are implemented in an interactive context with data-driven and collaborative analysis. This approach allows researchers and practitioners to evaluate their work and understand the underlying problem causes, enabling organizational change by implementing solutions. It was previously mentioned that based on the findings from the interviews and participant observation, a new and “transparent incident-reporting tool” was developed; it was then implemented at all ports in Mexico where the ISPS Code applies, by the National Maritime Authority. This demonstrated in a real case through “action research,” the contributions of this instrument to improve incident reporting, incident investigation,
Port Facility Security Assessments (PFSA), and Port Facility Security Plans (PFSP), as the ISPS Code requires. Measurements were done every quarter throughout the year 2017 and the incident-reporting instrument was adjusted accordingly when incidents without code were reported, adding new codes.

4 Results

On the basis of the interviews/observation, 15 themes were identified across the studied groups (CUMARs & UNAPROPs, Port Administration Directors; Maritime Customs Unit Directors; Port Security Officers (PSO) and Port Facility Security Officers (PFSO) and Harbor Masters). These issues affect port security either in a negative or positive way. It is also important to highlight that these findings were developed before the transferal of the National Maritime Authority from the MCT to MMAR, which entered into force on 17th of June 2017. However, the CUMAR was responsible for implementation and compliance of the ISPS Code since 21st of April 2014. These themes are the following:

1. High discontent among Maritime Customs Units Directors concerning the rotation of customs authority agents between maritime customs units, airport units, and cross-border units;
2. High reluctance by port administrations and PSO to allow port security authorities from the CUMARs and UNAPROPs permanent interconnection to CCTV systems in real time;
3. High reluctance by port terminals managers and PFSO to allow PSO and the UNAPROPs permanent interconnection to CCTV systems in real time from port terminals installations;
4. High reluctance by Maritime Customs Directors to allow port security authorities from the CUMARs and UNAPROPs permanent interconnection to CCTV systems in real-time concerning customs warehouse and other vulnerable customs areas;
5. Separate IT and CCTV systems rooms between Naval authorities and Customs authorities;
6. High reluctance by port terminals managers and PFSO to share their PFSP with the representatives from port security authorities from the CUMAR (responsible for inspection and approval of PFSP) in order to inspect it, revise it, and approve it and to develop the PSP details for MARSEC (maritime security) level 3, a responsibility of the CUMAR;
7. Poor development of maritime security exercises (that relate to level 3). These activities were performed without access to PFSP from port terminals [exercises to be conducted once every calendar year, with no more than 18 months between them];
8. Lack of human and material resources at the UNAPROPs to cope with the ISPS Code duties;
9. Poor development of PSPs. They only consider risks and threats in the common port areas, installations, and roadways within the port, but not within the port terminals, neither analyze the impact of security incidents of the terminals against
each other and particularly, specific high risks terminals against other considered of less risk.

10. Poor training of private security agents concerning port security risks and threats, as well as use of fire weapons.

11. Satisfactory level of cooperation between the maritime customs unit authorities and the UNAPROPS for inspection of goods and vessels at the customs warehouse with the ZVB system and other no intrusive security systems. The ZVB is a mobile screening system using X-ray for screening of cargo and vehicles. It uses a backscatter technology to provide photo—images of suspected objects within the cargo such as explosives, currency, drugs, psychotropic materials, forbidden chemicals, and trade-fraud items;

12. With the exception of one port, none existence of official records of port and maritime security incidents (before the implementation of the “transparent incident reporting tool”);

13. Non-existence of PFSP’s amendments officially requested by port security authorities following port security incidents;

14. Non-existence of official re-assessment of PSA/PSSA requested by port security authorities following port security incidents;

15. Non-existence of official investigation of port security incidents (other than the judicial one) made by port security authorities.

Concerning the implementation and results of the “transparent incident reporting tool,” the results demonstrate a significant improvement in reporting port security incident records, which increased from zero to 57 during the first year of the tool’s implementation. During the first quarter of 2017, 20 port security incidents were reported. For the second quarter of that year, the related figure was 9, which represented a decrease of 55.00%, compared to the first quarter. During the third quarter, a total of 17 port security incidents were recorded, which represents an increase of 88.88%, compared to the previous quarter. For the fourth quarter, 11 port security incidents were reported. This represents a decrease of 35.29%, compared to the previous period. In addition, 56% of the reported maritime incidents followed recommendations to be integrated into the PFSA and to be considered for improvement of PFSP. As it can be observed in Fig. 2, the type of security incident that was reported most is the code IFP-007, which relates to “confiscation of drugs, narcotics, or psychotropic material.” The second place is shared by the classification codes IFP-006 (confiscation of weapons/firearms); IFP-009 (unauthorized access to restricted areas, including fishermen and stowaways); IFP-017 (vehicles abandoned in the port installations or its surroundings); IFP-019 (failures in control areas); and the category “without code.” The last category served a special purpose: this type of incidents was assigned a code for the new quarter in relation to the period they were recorded (Fig. 3).

5 General discussion

A number of participants’ quotes are used to better illustrate the associated data. Concerning category (I), one of the quotes that better illustrates this is from one of the interviewed directors of maritime customs units, who pointed out that:
The rotation that exists, if it is not made in an integral way and I will clarify some points regarding the integral, the rotation is not very convenient; it can even be harmful for us. I mean that we have the specialization that some agents may be in a Border Customs Unit. Others may be entirely in an Airport Customs or a Maritime Customs Unit, the way of working in each of the points is definitely very different, huh! (…) But the frequency with which they are rotating the people sometimes is inadequate, or the type of people which they are sending to us in the rotations is also inadequate. There are some very special places, and I am going to say it clearly: The Northern border. If they send to us, if they send me an element of the northern border, since it arrives here, my hair starts to fall. I cannot generalize it, but it is a high percentage, which implies that I supervise it, if I have to supervise a person once, I have to supervise that particular person five times or more, then the rotation generates some complication. A rotation from an Airport Customs Unit to a Port Customs Unit is not so serious, the only problem is that it

![Fig. 2](image1)  
**Fig. 2** Graphic of port security incidents by quarter

![Fig. 3](image2)  
**Fig. 3** Graphic of port security incidents by incident code
slower the processes. It is the people coming from the border units, which have represented problems for us.

Regarding themes II, III, and IV, concerning high reluctance by port administrations and PSO, port terminals managers, and PFSO and Maritime Customs Units directors, respectively, to allow port security authorities from the CUMAR and UNAPROPs permanent interconnection to CCTV systems in real time, the following quotes illustrate the situation. “One representative from a UNAPROP said regarding the access to the CCTV from the Federal Integrated Port Administration (FIPA) installations,

We should have the management of the security cameras and CCTV systems, here in the Port, but we do not. The complete management of the CCTV system for the port is run by the port administration. We have something that is supposed to be a mirror of the CCV system here; but we are not connected to all the cameras; only to those that they allow us to have. In the case of a security incident in the areas that we are not connected to, with cameras, we get it recorded in DVR but that’s not in real time. It is after the event, so we do not know with certainty if the DVR has been edited.

Another agent of the UNAPROP from another port lamented the following concerning the PFSO collaboration to CCTV systems:

No, no, and no! In this case, when we made the last security exercise at level 3, the only port terminal that cooperated with us was one of containers, all the other ones denied us the access to their CCTV systems. Even that one, was very reluctant and its cooperation was not in real time. They brought with them a DVR with the records of the last week before the exercise (...). They did not give us access to the CCTV system because since they are private terminals, their general managers or CEO of the companies from Mexico City did not allow them. That is what they said.

On the other hand, one of the directors of the Maritime Customs Units said about the subject:

We are not allowed to do that. That would have to be negotiated in a higher level, at a minister level, I think. But until now they (the CUMAR and UNAPROP) have not requested access to our CCTV. However, I could not allow it, without discussing with the General Director.

These arguments might also be the reason for a separate IT and CCTV systems rooms between Naval authorities and Customs authorities at the ports, as represented by theme V.

This pattern about high reluctance of sharing CCTV systems in real time with the CUMARS & UNAPROPs was broadly shared across the studied groups and only in one case, port security authorities reported to have fully access to this system in real time for the common areas of port installations, excluding port
terminals and its related berths. A similar approach [to that for CCTV systems] was found regarding theme VI: “high reluctance by port terminals managers and PFSO to share their PFSP with representatives from the CUMAR (responsible for inspection and approval of PFSP). This in order to inspect it, revise it and approve it, (their duty by law) and to develop the PSP for MARSEC (maritime security) level 3 (responsibility of the CUMAR).” In the 100% of the cases, the port security authority’s representatives from the CUMAR and UNAPROPs reported that they did not have a copy of the PSP/PFSP for both the port and its terminals. In this regard, one of the quotes that best illustrate the identified problem is the following:

The Port Security Plan (developed by the PSO for the port), we have never seen it, we have one, but it is made by us. About their plan (Port Security Plan), I do not know if it is well developed, or which authorities do they include to attend security threats. I do not know if they include us, because they have never ever let me see it, and I have requested it many times. I know it is our responsibility to review it and they know it too, but they have their plan under four locks and they have not allowed us to see it. I have been asking for the PSP for two years. Personally, I have written here the Port Security Plan, but the one prepared by us for level 3, where I include Customs authorities, the port administration with its entire people, as it should be, and other local authorities; but until now, they have not let me see their PSP. Even when I have let them see ours for the practices and exercises in which we have participated, but they have not given me their plan or let me see how it is integrated. We have participated in all the practices they have done, but according to what they have requested at the time, because they have their own plan.

Concerning theme VII, “poor development of maritime security exercises at level 3, most performed without access to PFSP from port terminals”; another representative from the UNAPROPs said:

In the last exercise at level 3 made by the CUMAR it was requested the PSP to the PSO. He was also inquired in his character of PSO for the whole port, to gather the PFSP for the port terminals operating in the port. But the PFSO from the terminals denied to deliver it to him, I know it, because I saw when he requested it and they said no, only one of them accepted to show it to him but not to make a copy or to take it with him to the tactic room where the exercise was planned and implemented. I do not know... but the exercise was developed without any PFSP from the terminals.

Furthermore, all the interviewed representatives from UNAPROPs, the unit with duties of coast guard coincided in pointing out the lack of personnel, regarding theme VIII, “Lack of human and material resources at the UNAPROPs to cope with the ISPS Code duties,” one of the interviewed persons from the referred unit answered:
We lack personnel. I believe that here, at this UNAPROP we are not operating at 100%. No, because we do not have the 100% of the positions authorized for this unit, according to the organic personnel list. The organic list is for 43 elements and I do not have them. I have only three and 33 commissioned from the Infantry of Marina. In total, we are 36, but only half per shift.

Due to the high reluctance of the PFSOs to share their PFSP, the development of PSP is rather poor, since Port Security Officers mainly focused on risks and security threats for the common port areas, installations and roadways within the port, as the port assets. However, they do not include the different port terminals within their analyses, neither examine the impact of security incidents of terminals against each other and the rest of the port installations and particularly, specific high risks terminals against other considered of less risks (theme IX). Another critical subject is the theme X. Since most of PSO/PFSO do not have a military or police background, they lack training about use of fire weapons; as a result, they do not include this aspect in the performance evaluation of security drills. It was observed poor training of private security agents at 70% of the visited terminals with armed personnel when they were asked to assemble and disassemble their weapons and lock and unlock them. Therefore, it is necessary the cooperation with personnel from the UNAPROP to execute this type of security drills under a realistic approach. It is not a coincidence that according to the IMO, security drills, in general, shall be conducted every 3 months, to test individual elements of the PFSP, including the response to security threats, breaches of security and security incidents, taking into account the types of operations, personnel changes, the types of ships interfacing with the facility, and other relevant circumstances (International Maritime Organization 2012).

A subject that created high concern was about theme XII, “none existence of official records of port and maritime security incidents (before the implementation of the “transparent incident reporting tool”). All UNAPROP personnel interviewed concurred in the argument that there were no security incidents reported, because those that occurred were not considered serious. Despite this, it was observed and documented with photo-evidence through the visit to port installations and port terminals, situations where fishermen were within the navigation channels of the ports and at the berths of port terminals, as well as several unauthorized persons selling food at one of the ports. Personnel from the UNAPROPs were questioned about the issue and they answered that these people were not dangerous, so they were just invited to leave the place without further enquiries. Additionally, when they were questioned about cases of stowaways in ships or in the rail wagons within the port areas, one of them replied:

Yes, yes. But, it almost always has been by mistake, why? They usually do not aim to enter the port. Normally they are from Central America and they just want to go to the United States. They argue that they took the wrong train because they thought it was going to the North and they did not know that it was to enter the port. That they thought it was the “beast” and in that case, what we do is to deliver them to the National Institute of Migration, so they do what they have to
do according to their duties and responsibilities. There have been about four or five of these cases in the time that I am here (two years).

The port security incidents occurred at the different ports and port terminals were not considered serious enough to be recorded and therefore, there is an absence of PFSP’s amendments officially requested by port security authorities following port security incidents (theme XIII). Neither of official re-assessment of PSA/PSSA requested by port security authorities following port security incidents (XIV). Consequently, there is none existence of official investigation of port security incidents (no the judicial one) made by port security authorities or by the National Maritime Authority either (XV). To illustrate this theme, it was chosen the quote of one of the participants that best illustrate the situation:

Mmm, how to say it? “We make an informative letter about the control and situation of the port with the observations we have, in the sense of port security. Like certain areas that can serve to hide so they are more protected; but it is sent as an informative note, but officially request modifications to the port security plan on the bases of our observations, or findings, no.

This instrument combined with the use of statistics by incident code and port/port facility, at a macro level, provides the State with crucial information to set up strategies for developing a National Maritime Security Policy. It allows the State to clearly identify threats and allocate material, economic, and human resources accordingly, as required at each port, applying a risk-based approach to port and maritime security management. It bears emphasis that “the intangible security assets and management of those assets or the way regulation is implemented that can make the most difference” (Mileski et al. 2015) in the benefits that may accrue to all concerned from effective port and maritime security.

Although this instrument was successfully implemented and tested at all ports where the ISPS Code applies, in Mexico, with most type of port facilities, it can easily be adapted to other countries facing the same problems worldwide, recognizing that the “safety and security of maritime domain are critical aspects for sustainable development” (Chintoan-Uta and Ramos Silva 2017). It can also be modified to include other type of incidents not considered in the format by adding the type of security incident and allocating the respective incident code.

Edgerton (2013), cited by Kusi (2015), said that when security strategies and measures are appropriately designed, functions as enablers, facilitating cost-effective and reliable operations for all stakeholders.

6 Conclusions

The maritime security standards in Mexico, concerning security incident reporting, inspections and revisions to PSA/PFSA, prior to the transferral of the Maritime National Authority from SCT to SEMAR in June 2017 was rather poor. Yet, SEMAR was responsible for maritime security since the 21st of April, 2014 when the presidency of the CUMAR was transferred from Masters of Harbors to
Admirals, Commanders of the Navy sector, zone or region for the specific port. Commanders of the Navy at the zone in the different ports before this reform were appointed as vice-presidents of this Unified Centre for Maritime Security, according to the Law of Ports. However, because of lack of knowledge and poor training, they were not fully aware of the changes and their new responsibilities, which resulted in the fact that port and maritime security duties (concerning the ISPS Code), were rather neglected.

On the positive side, important solutions were implemented in 2017. ISPS Code related training was provided by appropriate qualified people, to members of the CUMARs and UNAPROPs; the National Maritime Authority also implemented the “transparent incident-reporting tool” at all ports of the country. This brought a significant improvement on reporting of incident security incidents and updating of incident security records, during the first year of its implementation. Moreover, 56% of the reported incidents were followed with recommendations to be considered for PSA/PFSA and PSP/PFSP. Slowly but surely, the port and maritime security in Mexico is improving in a significant way and the country is getting ready to exploit in a safer and secure manner; it’s more of 11,000 km of coastline both on the Pacific and Atlantic oceans through its ports and related infrastructure.

7 Future research areas

Further research in this topic include examining the implementation of the CUMAR and UNAPROPs recommendation to the PSA/PFSA and PSP/PFSP, as well as the development of security incident-reporting in the country. This might be done by developing statistics, using the 2017 figures as weight for next years.

Other areas include necessary law reforms to integrate the part of the ISPS Code (SSO, SSA and SSP) that currently are not reflected in the CUMAR’s Regulation.

Acknowledgements  It is necessary to acknowledge the support of the National Maritime Authority in Mexico, the Secretary of SEMAR, Admiral Vidal Francisco Soberón Sanz, towards the implementation of the incident-reporting tool and access to the setting. Grateful thanks are also appropriate to Admiral Ángel Enrique Sarmiento Beltrán, Under-Secretary of SEMAR, for his willingness to discuss the implementation of the incident-reporting tool, its benefits and opportunities for improvement during the action research study.

Many thanks are also appropriate to those participants interviewed at the Maritime Customs Units, Master of Harbors; Port Administration Directors; Port Security Officers; Port Facility Security Officers, Commander of the Navy functioning as presidents of the CUMAR at the visited ports and commander of the UNAPROPs.

Abbreviations  AIS, automatic identification system; CCTV, closed-circuit television; CI Code, code of the international standards and recommended practices for a safety investigation into a marine casualty or marine incident; CSO, Company Security Officer; CSR, continuous synopsis records; CUMAR, Centro Unificado para la Protección Maritima y Portuaria and represented with the abbreviation “CUMAR,” in Spanish (Unified Centre for port and Maritime Security, Mexico, own translation); DOF, diario oficial de la federación, in Spanish (official diary of the federation, in English); DoS, declaration of security; EEZ, exclusive economic zone; FIDENA, Fideicomiso de Formación y Capacitación para el Personal de la Marina Mercante Nacional, in Spanish, in Mexico (Fund of Education and Training for the National Merchant Marine, in English, own translation);IMO,
International Maritime Organization; *ISM*, International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code); *ISPS Code*, International Ship and Port Facility Security Code; *ISSC*, International Ship Security Certificate; *PFSA*, Port Facility Security Assessment; *PFEO*, Port Facility Security Officer; *PFSP*, Port Facility Security Plan; *PSA*, Port Security Assessment; *PSAC*, Port Security Advisory Committee; *PSO*, Port Security Officer; *PSP*, Port Security Plan; *RGO*, Recognized Security Organization; *SCT*, Secretaría de Comunicaciones y Transportes, in Spanish, Mexico (Secretariat of Communications and Transportation); *SEMAR*, Secretaría de Marina, in Spanish, Mexico (Secretariat of the Navy); *SOC*, statement of compliance; *SOLAS*, International Convention for the Safety of Life at Sea, 1974; *SSA*, ship security assessment; *SSAS*, ship security alert system; *SSO*, Ship Security Officer; *SSP*, ship security plan; *STCW*, International Convention on Standards of Training, Certification and Watch keeping for Seafarers, 1978; *SUA*, convention for the suppression of unlawful acts against the safety of maritime navigation, protocol for the suppression of unlawful acts against the safety of fixed platforms located on the continental shelf; *UN*, United Nations; *UNAPROP*, Unidad Naval de Protección Portuaria, and represented with the abbreviation UNAPROP, in Spanish, in Mexico (Navy Unit for Port Protection, own translation); *UNCLOS*, United Nations Convention on the Law of the Sea of 10 December 1982; *WCO*, World Customs Organization

**References**


International Maritime Organization (2014) Model course 3.11 safety investigation into marine casualties and marine incidents. IMO


