Legal analysis on Cambodia regulation apply to ISPS Code

Chanveasna Teth
WORLD MARITIME UNIVERSITY  
Malmö, Sweden

LEGAL ANALYSIS ON CAMBODIA  
REGULATION APPLY TO ISPS CODE  

By

TETH CHANVEASNA  
Cambodia

A dissertation submitted to the World Maritime University in partial fulfilment of the requirements for the reward of the degree of

MASTER OF SCIENCE  
in  
MARITIME AFFAIRS  
(MARITIME LAW AND POLICY)  

2020

Copyright Teth Chanveasna, 2020
Declaration

I certify that all the material in this dissertation that is not my own work has been identified, and that no material is included for which a degree has previously been conferred on me.

The contents of this dissertation reflect my own personal views, and are not necessarily endorsed by the University.

(Signature): (Date): 2020/09/24

Supervised by: Dr. Carolina Romero
Supervisor’s affiliation: MLP
Acknowledgement

First of all, I would like to thank Professor Carolina Romero for providing me the valuable advice on methodology and facilitating me to achieve this dissertation. Without her help and support, I may not finish this research.

Secondly, my deepest thanks to a donor from the International Maritime Organization that provided me an opportunity to study Master of Maritime Science, Specialization Maritime Law and Policy at World Maritime University. At the same time, I am not only thankful to all professors that taught me at World Maritime University but also thankful to the President, Vice president, Head Specialization of MLP and Staff of World Maritime University.

Thirdly, I would like to extend my heartfelt gratitude to leaders, managers and officials of Phnom Penh Autonomous Port that gave me a chance to study at World Maritime University.

Lastly, I cannot forget my beloved parents, Cambodian families in Malmö, Sweden and friends that always motivated me to study hard and achieve this study.
Abstract

Abstract Title of Dissertation: Legal Analysis on Cambodia regulation apply to ISPS Code

Degree: Master of Science

The event of 9/11 was caused by a terrorist attack at the World Trade Center in New York, USA, led to thousands of people to losing their lives and caused a huge impact on the economy of the country. Consequently, ports and ships were considered to be vulnerable targets of terrorist attacks as well as potential means of attack. In this sense, in order to protect port facilities and ships from terrorist attacks, the International Maritime Organization amended SOLAS Chapter XI-2 and adopt a new regulatory regime for maritime security by way of the ISPS Code. Cambodia is a contract party to SOLAS Chapter XI-2. Therefore, it needs to apply and comply with the requirements of the ISPS Code in terms of maritime security. Therefore, this dissertation will undertake a legal analysis of the international obligation related to maritime security under the ISPS Code and the national obligations of Cambodia related to maritime security. This dissertation will contribute to understanding of the harmonization and/or conflict between international and national obligations related to maritime security. It also looks at the available implementation and difficulty in implementing the national obligations of Cambodia in compliance with international obligations related to maritime security. Finally, it is found that national obligations derived from regulations of Cambodia related to maritime security have harmonization with international obligations derived from the ISPS Code. However, the national obligation deriving from the national law of Cambodia related to maritime security is not yet in effect for all ports involved in international trade. This dissertation provides recommendations to the ports of Cambodia that interact with international trade to comply with the requirement of the Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security adopted on December 20th 2017.
Contents

Declaration .......................................................................................................................... 2
Acknowledgement ................................................................................................................ 3
Abstract .............................................................................................................................. 1
Contents ............................................................................................................................. 6
List of Figure ....................................................................................................................... 9
List of Table ........................................................................................................................ 10
Abbreviation ....................................................................................................................... 11
Chapter 1. Introduction ...................................................................................................... 12
  1.1. Background .............................................................................................................. Error! Bookmark not defined.
  1.2. The problem statements ......................................................................................... Error! Bookmark not defined.
  1.3. Motivation ................................................................................................................ Error! Bookmark not defined.
  1.4. The objective of research .................................................................................... Error! Bookmark not defined.
  1.5. Research questions ............................................................................................... Error! Bookmark not defined.
  1.6. Theoretical framework ......................................................................................... Error! Bookmark not defined.
  1.7. Methodology .......................................................................................................... Error! Bookmark not defined.
  1.8. Structure of dissertation ...................................................................................... Error! Bookmark not defined.
  1.9. Timelines ................................................................................................................. Error! Bookmark not defined.
  1.10. Expected results .................................................................................................. Error! Bookmark not defined.
  1.11. Key assumptions and Limitations ....................................................................... Error! Bookmark not defined.
Chapter 2 .......................................................................................................................... 20
  2.1. Concept of Maritime Security .................................................................................. 20
2.2. Unclose 1982 Regime ................................................................. 23
2.3. SUA Convention Regime .......................................................... 24
2.4. Maritime Security in Cambodia .................................................. 26
  2.4.1. Background of Cambodia .................................................... 26
  2.4.2. Contemporary maritime issue of Cambodia ................................ 26
  2.5. Summary .................................................................................. 28
Chapter 3 ...................................................................................... 29
  3.1. Contract government obligation .............................................. 29
  3.2. Ship operator responsibility ..................................................... 31
    3.2.1. Ship security assessment .................................................... 32
    3.2.2. Ship Security Plan .............................................................. 32
    3.2.3. Company Security Officer ................................................. 33
    3.2.4. Ship Security Officer .......................................................... 34
  2.3. Port facilities operator responsibility ...................................... 35
    3.3.1. Port Facility Security Assessment ....................................... 35
    3.3.2. Port Facility Security Plan .................................................. 36
  3.4. Summary .................................................................................. 37
Chapter 4 ...................................................................................... 38
  4.1. Legal Framework ..................................................................... 38
  4.2. Maritime administration ........................................................ 39
  4.3. Recognized Security Organization .......................................... 41
  4.4. National Obligation of Port Facility Operator ......................... 43
    4.4.1. Port facility Security Assessment ........................................ 44
List of Figure

Figure 1: Structure of general Department of water Maritime Transport and Port .......... 41
List of Table

Table 1: Matrix of Maritime Security .................................................................23
Table 2: Legal framework of Cambodia relate to Maritime security .......................39
Table 3: Recognize Security Organization ............................................................43
Table 4: Port Facility Security Assessment ..........................................................45
Table 5: Port Facility Security Plan ........................................................................48
Abbreviation

Company Security Officer (CSO)
General Department of Waterway and Maritime Transport, and Port (GDWTP)
International Ship and Port Facility Security Code (ISPS Code)
Ministry of Public Work and Transport (MPWT)
Port Facility Security Plan (PFSP)
Port Facility Security Assessment (PFSA)
Port Facility Security Officer (PFSO)
Ship Security Plan (SSP)
Ship Security Assessment (SSA)
Ship Security Officer (SSO)
Recognize Security Organization (RSO)
Chapter 1. Introduction

1.1. Background

Maritime security is a well-known concept in international relations. Ocean governance and international security play important roles in maritime policy. Legal framework and policy on maritime security were done by states worldwide, such as the United Kingdom, European Union, African Union and the USA. In 2011, Maritime Security was one of The North Atlantic Treaty Organization (NATO)’s priority objectives under its Alliance Maritime Strategy. The U.S.A. also developed a national Maritime Security Policy in 2004 (Bueger, 2015). Meanwhile, IMO applies the term maritime security that refers to its member stat’s ability to protect civil maritime stakeholders such as shipping and port sectors from threats and help the government protect global maritime trade (IMO, 2020). Furthermore, maritime security is also defined as acts that are unseaworthy of seaborne trade. The common causes of maritime insecurity are piracy, armed robbery, terrorist acts, illegal trafficking of arms and weapon of mass destruction, illegal trafficking of narcotics and persons, illegal fishing and criminal damage to the marine environment (Bueger, 2015). An often-cited example of terrorism at sea is the hijacking the Italian cruise ship ACHILLE LAURO by an armed group of people from Palestine on October 07, 1985. They seized 400 crew and passengers on board by threatening to kill them and demanded that an Israel release a number of Palestinians held in prison there. When the demand was not met one day later, the hijackers killed a disabled, elderly Jewish man as the warning to Israel. This incident led to IMO taking into account that crew, passengers and cargo may be endangered by terrorist acts, which was a new threat to maritime security in addition to traditional dangers such as piracy and armed robbery. On this basis, IMO adopted the 1988 Convention to suppress unlawful acts against the safety of maritime navigation, hereafter called the 1988 SUA Convention. The 1988 SUA Convention has the main purpose of providing effective and practical measures to prevent unlawful acts against the safety of maritime navigation, and to prosecute and punish perpetrators
(Mensah, 2004). However, after the events of September 11, 2001, besides the safety of maritime navigation, the port sector became a focus of maritime security.

These attacks raised awareness of the vulnerability to terrorist attacks of all modes of transportation. It was recognized that ports, cargo ships and cruise ships could be used by terrorists to perpetrate attacks on U.S. citizens. Therefore, port security in the U.S. has become stronger and improved by significant regulation. Legislators in the U.S. adopted a significant policy, S.1214, in November 14, 2002, to respond to and prevent the events of 9/11 from happening again in the USA (Fritelli, 2005). Internationally, the terrorist attacks of September 11, 2001 prompted huge concerns about maritime security. IMO undertook to revise the 1988 SUA Convention to address the new problem raised by the events of September 11/2001 by considering two main issues. Indeed, those issues exist to develop effective measures to prevent ships from being used as means or support for terrorist activities and to ensure that perpetrators of violent acts at sea are brought to justice (Mensah, 2004). After that, IMO amended the 1974 SOLAS Convention and adopted the International ship and port facility security (ISPS) Code on December 12, 2002, by the Conference of Contracting Governments to the SOLAS, 1974. The ISPS Code entered into force under SOLAS chapter XI-2 on July 01, 2004.

The ISPS Code has the main purpose of setting comprehensive measures to enhance the security of ships and port facilities and respond to threats to ship and port facilities. The ISPS Code is divided into two parts: Part A is mandatory and part B is non-mandatory. Part A provides an outlined framework for contracting governments, shipping companies and port authorities to comply with the ISPS Code. At the same time, Part B offers recommendations and guidelines to implement mandatory part A of the ISPS Code. Furthermore, the ISPS Code provides the scope of work to detect potential security threats to ships and port facilities. In this sense, the responsibilities of all stakeholders concerned with maritime security in ports and onboard ships are under the provision of the ISPS
Code. Besides, the ISPS Code aims to ensure efficient collation and exchange of maritime security-related information (IMO, 2020).

In terms of maritime security, Cambodia has ratified international regulations such as SOLAS, MARPOL, and STCW (Japan International Cooperation Agency, 2007). Cambodia implements the ISPS Code as part of SOLAS. In order to comply with the ISPS Code, which is the international regulatory framework for maritime security, Cambodia adopted Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security on May 09, 2006. As stated in the article 1, the Sub-Decree # 40 (RGC) has the main objective to control the ship and port facility security of the Kingdom of Cambodia through international cooperation with the contracting governments, shipping companies, and the ports regarding sea-going transport. Furthermore, according to article 6 of the Sub-Decree # 40 (RGC), the Ministry of Public Work and Transport (MPWT) has the competency to control ships and port facilities' security. At the same time, the Management Committee for Cambodian Ship Registry (MCCSR) has competency to control Cambodian ships' security. Moreover, Sub-Decree # 40 (RGC) has the scope of work over the ships that operate international navigation as the priority of all kinds of passenger ships, cargo ships loading a total volume of over 500 GT. However, this Sub-Decree does not apply to military vessels, State ships that are not affiliated with business or military ports. At the same time, as stated in article 7, the Sihanoukville Autonomous Port (SAP) and Phnom Penh Autonomous Port (PAP) or other International Ports of the Kingdom of Cambodia shall be defined by the Royal Government to comply with the Sub-Decree # 40 (RGC). Furthermore, on December 20, 2017, the Ministry of Public Work and Transport (MPWT) issued a regulation called Prakas No 432 BK on the port facilities of Cambodia to implement Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security, adopted on May 09, 2006.
1.2. The problem statements

Cambodia is a contracting party to SOLAS chapter XI-2. Therefore, Cambodia needs to have national obligations related to maritime security as required by the ISPS Code.

1.3. Motivation

The author has been working for Phnom Penh Autonomous Port since 2013. The author would like to build and expand knowledge of port law, port policy and port administration and serve Cambodia's port sector. Cambodia is a developing country and wants to modernize its economy, infrastructure, laws and regulations, administration, technology and human capacity to have international standards. The maritime security sector of Cambodia also needs to improve based on the international standard. The ports of Cambodia can participate to promote stability of the global maritime security. Therefore, the author is motivated to study this topic to understand the maritime security threats to port facilities.

1.4. The objective of the research

This research has a basic objective:
- To analyze international obligations related to maritime security derived from the ISPS Code.
- To analyze national obligations related to maritime security derived from the national law of Cambodia.
- To analyze both international obligations derived from the ISPS Code and national obligations derived from the national law of Cambodia to see whether international and national obligations related to maritime security are in harmony or in conflict with each other.
1.5. Research questions

1. What is the international obligation related to maritime security derived from the ISPS Code to contract parties, the shipping industry, and port stakeholders?
2. What is the national obligation related to maritime security derived from the national regulation of Cambodia?
3. Are the international obligations related to maritime security derived from ISPS Code and the national obligations derived from Cambodia's national law related to maritime security inharmony or in conflict?

1.6. Theoretical framework

Firstly, the author will analyze the international obligation of the contracting party, shipping and port operator related to maritime security derived from the ISPS Code. Secondly, the author will analyze national obligations of the maritime administration, ship and port facilities related to maritime security derived from Cambodia's national law. Thirdly, the author will analyze the international obligations derived from the ISPS Code and national obligations derived from Cambodia's national law to see whether international and national obligations related to maritime security are in harmony, similar, or in conflict with other. Simultaneously, the author also analyzes Cambodia's national obligations to see which obligations are available and easy to implement and which obligations are difficult to implement. Lastly, the author will conclude the national obligations derived from national law that are not harmonized with the international obligation derived from the ISPS Code or are difficult to implementing.

1.7. Methodology

Firstly, the author will analyses the ISPS Code to determine the international obligations of the contracting party, shipping and port sectors related to maritime security. Secondly, the author will analyses the Sub-Decree # 40 (RGC) on Vessel Security and Port Facility
Security on May 09, 2006; and Prakas No 432 BK on the port facilities on December 20, 2017 of Cambodia to determine the national obligations of the maritime administration, shipping and port sectors related to maritime security.

1.8. Structure of the dissertation

Chapter 1. Introduction

Chapter 1 consists of the background, problem statement, objective, research question, theoretical framework, methodology of research and structure of dissertation, expectation result and limitation of the dissertation.

Chapter 2. Literature Review

In chapter 2, firstly, the author will review the previous research related to the concept of maritime security, and the SUA Convention regime; and secondly, the author will review previous research related to maritime security in Cambodia which consists of the background of Cambodia and contemporary issues of maritime security in Cambodia.

Chapter 3. International obligation relates to maritime security derived from ISPS Code

Chapter 3 consists of background of the ISPS Code regime, and the international obligations of contracting parties, shipping and port operators related to maritime security derived from ISPS Code

Chapter 4 National obligation related to maritime security derived from national law of Cambodia

Chapter 4 discusses the legal framework, maritime administration, designated authority, national obligation of ship operators and port facilities of Cambodia related to maritime security.

Chapter 5. Legal Analysis between international obligation and national obligation

Chapter 5 consists of a legal analysis of the harmonization, conflict and implementation of national obligations related to maritime security by comparison with international obligations.
Chapter 6 Conclusion and recommendation

Chapter 6 consist of conclusion and recommendation based on the national obligations derived from national law which are not harmonization with the international obligations derived from ISPS Code and the difficulty implementing such obligations.

1.9. Expected results

This research will contribute information to the General Department of Waterway and Maritime Transport and Ports of the maritime administration of Cambodia, Sihanouk Autonomous Port and Phnom Penh Autonomous Port and shipping industrial to raise awareness of the international obligations and national obligations related to maritime security. Lastly, it is hoped that this research will contribute to the basic understanding of the maritime security obligations at the international level and national level of Cambodia for the public, academia and students.

1.10. Key assumptions and Limitations

Firstly, for Key assumption, this topic mostly focuses on international obligations and national obligations related to maritime security, maritime security measures, maritime administration, ship facility security plan, ship facility security assessment and ship facility security officer, port facility security plans, port facility security assessment and port facility security officer, port security measure; and ISPS Code.

Secondly, for limitation, the author had tried to access on the data of Sihanouk Autonomous Port on Port Facility Security Plan by sent email to them several times but the author could not get any feedback from them. Furthermore, the author also sent email several times to access the data from the General Department of Waterway and Maritime Transport, and Port of the Ministry of Public Work and Transport (MPWT) on Phnom Penh Autonomous Port and Sihanouk Autonomous Port relate to Port Facility Security.
Assessment and Port Facility Security Plan compliance to The Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security was adopted on May 09, 2006 and the Prakas No 432 BK on the port facilities of Cambodia was adopted on December 20th 2017 but the author did not get any feedback from them. However, the author can only access the Port Facility Security Plan of Phnom Penh Autonomous Port as the case study of this dissertation. In this sense, due to the lack of data relate to the real implementation of ISPS Code implantation in Cambodia, therefore, the author would like to do only legal analysis on the regulation of ISPS Code related to the international obligation of maritime security and regulation of Cambodia related to national obligation of maritime security.
Chapter 2

Literature Review

This dissertation has a purpose to analyze between international obligations derived from the ISPS Code and national obligations derived from the national law of Cambodia related to maritime security to see whether the two are harmonized, similar or in conflict with each other. In this sense, a literature review of previous research related to maritime security at the international level and at the national level of Cambodia is undertaken in this chapter of this dissertation (Knopf, 2006).

2.1. Concept of Maritime Security

The concept of maritime security has been discussed with the intent to provide a definitive meaning; however, an agreed definition of maritime security has not been reached. There is disagreement on the meaning of maritime security because one side defines it as the absence of threat to the sea zone, while the other side defines it as good or stable order at sea. The threat to the sea zone consists of maritime inter-state disputes, maritime terrorism, piracy, trafficking of narcotics, people and illicit goods, arms proliferation, illegal fishing, environmental crime, and maritime accidents or disaster. Opposite to the meaning of threat, the absence of threat is good or stable order at sea. At the same time, the absence of threat is also referred to in the positive meaning of maritime security that links to economic or blue growth, which benefit from the stable order at sea.

Furthermore, the meaning of maritime security can be determined from the traditional concept and beyond the traditional concept (Bueger, 2015). The traditional understanding of maritime security is derived from the concept of sea power and maritime safety. The concept of sea power refers to the geopolitical and geostrategic interests of states and
regional organization. This concept also remains inside the national security of states, consisting of inter-state disputes, terrorist acts and arms proliferation. For example, the inter-state dispute on territorial sea claims in the South China Sea showed the geopolitical power of the state to claim its interest in the sea base on their power of military (Stockbruegger & Bueger, 2014). The concept of maritime safety that considers maritime accidents and climate change is also linked to maritime security. For instance, the oil spill from the event of the 1991 Gulf War had links to traditional maritime security and environment concerns. However, a new concept of maritime security is established by relying on the inter-relationships of the concepts of sea power, maritime safety, blue economy and human resilience. The concept of blue economy is related to the economic benefits of the ocean derived from shipping, and living and non-living resources. Lastly the concept of human resilience refers to the food security derived from the blue economy. For example, fish stock serves as food security for human beings. Even though the new concept of maritime security intends to integrate the four concepts, this definition is still not fully accepted as the harmonized definition of maritime security (Bueger, 2015).

However, the common internationally accepted definition of maritime security based on its daily use refers to piracy and armed robbery, terrorist acts, illegal trafficking of arms and weapons of mass destruction, illegal trafficking of narcotics and persons, illegal fishing, and intentional and unlawful damage to the marine environment (Roach, 2004). At the same time, piracy and armed robbery is clearly defined as the traditional threat to maritime security, while terrorist acts are considered as the new threat to maritime security (Mukherjee, 2007). For example, in the Law of the Sea 1982 regime, piracy was clearly defined and, consequently, piracy refers to any illegal acts committed by the private interest group of people against or attack ship or crew while ship and crew in the maritime area. On the other hand, terrorism refers to the political behavior of adversaries by attacking and threatening targets that process symbolic rather than material significance. The cause of terrorism act is motivated by political intent, while piracy is motivated by
the interests of one group of people (Mensah, 2004). Even though, piracy and terrorist acts have different meanings, the solutions to both problems were learned from one to another and interaction with each other. For example, the solution to piracy acts was provided by the UNCLOS 1982 regime in its article 100 as stated that all states have a duty to cooperate to the fullest possible extent in the repression of privacy on the high seas or in any other place outside the jurisdiction of any state (UNCLOS 1982). Moreover, IMO adopted regulation as a consequence of piracy and terrorist acts by creating the 1988 SUA Convention as the prevention measure for all unlawful acts against the safety of maritime navigation (Mensah, 2004). Later on, MO adopted the ISM Code for maritime safety management and the ISPS Code for maritime security measures (Mukherjee, 2007).

In conclusion, the concept of Maritime security that has been discussed in different papers. It can be defined as the threats to the order at sea, whether the threat is the traditional threat such as the piracy and armed robbery, or a new threat such as terrorism. Moreover, the threat has led international actors such as the IMO to adopt solutions to those threats by providing duties and responsibilities to all related stakeholders to protect themselves from those threats. In this sense, it is seen that there are three international law regimes, UNCLOS 1982, the 1988 SUA Convention and the ISPS Code of SOLAS that aim to provide a solution to the threats to maritime security.
Table 1: Matrix of Maritime Security

Source: Bueger (2015). What is maritime security?

2.2. UNCLOS 1982 Regime

The UNCLOS 1982 regime has covered the common traditional problems that threaten maritime security. Those problem consist of illegal human trafficking, piracy and robbery, and illicit trafficking of narcotic drugs or psychotropic substances. For instance, as stated in article 99 on the prohibition of transport of slaves, each state should take measures to protect, punish and ban those ships that fly their flag to transport slaves illegally. Furthermore, article 99 also requires the flag state to take measures to prevent unlawful use of its flag by ships in order to transport slaves. Besides human trafficking, according to article 100 of UNCLOS, every state needs to facilitate cooperation on the suppression of piracy on the high seas or any place outside the jurisdiction of states. In this sense, the state has an obligation to cooperate in dealing with the problem of traditional threats to maritime security namely piracy and armed robbery. Moreover, the UNCLOS 1982 regime has defined the meaning of piracy for state suppression and combating. The
definition provided by UNCLOS in article 101 is any illegal act with violence and detention or depredation that committed to the crew, passenger or ship by private purpose of a group of people at the high sea or outside jurisdiction of state. In addition, any act of voluntary participation in the operation of a ship or aircraft with knowledge with the purpose to pirate ship or aircraft were defined as the piracy threat to maritime security. Lastly, according to article 108, every state is required to cooperate in order to suppress the illegal act of trafficking narcotic drugs and psychotropic substances engaged by ships in the high seas that violate international law. Article 108 also provides authority to the state to ground the ship, if the state believes that a ship that flies their flag is engaged in an illegal act of trafficking narcotic drug and psychotropic substances.

To sum up, the UNCLOS 1982 has defined the common traditional problems that threaten maritime security, such as illegal human trafficking, piracy and armed robbery; illegal trafficking of narcotics psychotropic substances and sets the obligation and responsibility of states to combat those problems.

2.3. SUA Convention Regime

The SUA convention was created in 1988 in order to provide effective and practical measures for the prevention of all unlawful acts against the safety of maritime navigation; and prosecution and punishment of perpetrators. In the SUA convention, the act of violence against a person on board a ship, destroying the ship or causing damage to the cargo on the ship, and placing on board a ship a device or dangerous substance that endangers the safe navigation of the ship are commonly identified a threat to maritime security (Mensah, 2004). Furthermore, serious attacks on ships such as hijackings planned by international crime organizations to steal the ship and its cargo are covered by the 1988 SUA convention. To confront those threats, states are provided with obligations to punish and sentence offenders that endanger the safety of maritime navigation of ships in their
territorial seas or ships that fly their flag under their own national jurisdiction court and law. For example, the MV Petro Ranger was hijacked in April 1998 by perpetrators from Indonesia off the coast of Malaysia. MV Petro Ranger was owned by Singapore nationals and flew the flag of Malaysia. However, this case is under the jurisdiction of China’s national law and court because MV Petro Ranger reflagged to the Honduran flag and changed its name to MV Wilby. But according to the 1988 SUA Convention, Malaysia and Singapore also have jurisdiction over the case of MV Petro Ranger. In the wake of the 9/11 incident, the 1988 SUA convention was updated to address the new problem and adopted the 2005 SUA protocol in April 2005. In the new update, the 2005 SUA protocol classifies two main categories as threats to maritime security, which consist of acts of maritime terrorism and nonproliferation offenses; one category relates to a new tool for punishment of the act of illegal transport of WMDs by ship in the high seas. First, the act of maritime terrorism refers to using a ship as a weapon or as a means to carry out a terrorist attack for the purpose of destroying or intimidating the governments or states. The act of maritime terrorism leads to endangerment of international maritime navigation. Second, nonproliferation offenses refer to the trafficking on the high seas in commercial ships of WMD. In this sense, the state party requires criminal transport on the high seas of WMD and certain related material. Last, the new tool to combat the proliferation of WMD was created as a response measure required by the UN Security Council. However, in order to protect the innocents such as crew and master, the new offenses of nonproliferation require knowledge and intent to traffic the WMD (Beckman, 2008).

To sum up, the 1988 SUA Convention and its new update the 2005 SUA protocol are a key to protect navigation of ships from the threats such piracy, terrorism or use of ships to illegally transport WMD. At the same time, every member state of the 1988 SUA convention has the right to use their own legal framework such as legal punishment to combat those threats. In this sense, the duty of each state to combat the threat of maritime security seems not to lack harmonization among the member states. Therefore, IMO
adopted the ISPS Code with the intent to make harmonization an obligation to protect the threat to maritime security (ISPS Code 2004).

2.4. Maritime Security in Cambodia

2.4.1. Background of Cambodia

Cambodia is located in the south-western part of the Indochina peninsula, Southwest Asia. Today, Cambodia has a land area of 181,035km², with a maximum length of the of 575 km in the east/west direction and 446 km in the north/south direction. Cambodia has borders with Laos and Thailand to the north and west, and with Vietnam to the southeast. Cambodia has a coastline within a length of 435km at the southwest border, which is confronted with the Gulf of Thailand. Cambodia has an extensive river system that consists of the Tonle Sap, the Bassac River and the Mekong River system that flows from the north to south in the midst of the Central plain. Cambodia is still densely forested in the highlands (JICA-Part 1, 2007).

2.4.2. Contemporary maritime issue of Cambodia

First of all, in the context of maritime security, Cambodia is a contract party to the fourth 1958 Geneva Convention on the Law of the Sea and is also a party to the Optional Protocol concerning the Compulsory Settlement of Disputes in 1970. Furthermore, Cambodia is a signatory country to the 1982 United Nations Convention on the Law of the Sea since 1983. Currently, Cambodia may access the exclusive economic zone within an area of 55,600 km² in the Gulf of Thailand (WEPA, 2020). Furthermore, to enjoy benefits from the sea, as stated in Article 56(1.a) of UNCLOS 1982 on the rights, jurisdiction and duties of the coastal State in the exclusive economic zone, Cambodia has sovereign rights for the purpose of exploring and exploiting, conserving and managing the natural resources of its
exclusive economic zone. However, Cambodia’s seas are vulnerable to security threats such as terrorism and transnational crime. There are a number of potential maritime security issues such as maritime border issues, infiltration of illegal fishing, and loss of maritime resources (Chap Sotharith, 2007). Moreover, common security threats are illegal fishing, human and drug trafficking, terrorism, piracy, transnational crimes, environmental degradation, and sea level rise (Chheang Vannarith, 2010). In this sense, the vulnerability to maritime security issues may lead to Cambodia losing large numbers of benefits from business on the sea such oil exploration, marine resources and seaborne trade. Consequently, the National Committee on Maritime Security was created in 2009 to enhance maritime security and strengthen the enforcement of rules and order at sea. However, maritime security threats such as an illegal fishing, transnational organized crime committed at sea and threats to the marine environment are still considered as the main problems in Cambodia. At the same time, lack of financial and human resources is also a key problem that leads to maritime security threats. Moreover, the weakness of the legal framework and coordination of relevant ministries are also issues affecting maritime security. The infrastructure and military assets such as battleships, combat boats and vessels are significantly important to protect from threats such as piracy, terrorism and any criminal acts against maritime security (Sotharit, 2018). In order to solve this problem, first, Cambodia shall develop legal procedures and framework by working together within the relevant ministries; second, it would be strengthen on the capacity of naval forces to enhance closer cooperation with related agencies to provide security and safety for economic activities; third, it would be strengthen on the cooperation with other countries to define the common maritime issues and find solutions; and lastly, it would be safeguard the resources within the territorial water and exclusive economic zone (Cambodia’s Defense White Paper 2006).

Lastly, the port sector is also considered as the one main factor contributing to maritime security. The ISPS Code has the main purpose to enhance security for ships and ports in
the context of maritime security. In Cambodia, the port sector is developing according to the regional and international’s favors. However, the port sector in Cambodia still has a lot of challenges such as compliance with international conventions and an issue of port administration and legal framework. For instance, Cambodia still lacks measures against oil spill contingency; lacks a framework for simplifying port procedures; has a complicated port administration system; lacks a national port policy, necessary for consistency with national land and economic; has difficulty reflecting the port sector viewpoint into port development; and lacks national information and data on port activities (JICA-Part 3, 2007).

2.5. Summary

To sum up, firstly, the concept of maritime security was defined based on its common uses, such as the threat to maritime security caused by piracy and armed robbery, terrorist acts, illegal trafficking of arms and weapons of mass destruction, illegal trafficking of narcotics and persons, illegal fishing; and intentional and unlawful damage to marine environment (Roach, 2004). Secondly, the contemporary challenges to the maritime security of Cambodia are piracy, terrorism and criminal acts at sea (Chheang Vannarith, 2010). Lastly, Consequently, doing on the literature review on the previous papers related to this dissertation topic found that there had not yet any papers discussed about ISPS Code implementation in Cambodia. Therefore, the topic of this dissertation on legal analysis on Cambodia’s regulation apply to ISPS Code is a new topic.
Chapter 3

International Obligations related to maritime security derived from ISPS Code

The new regime of the ISPS Code has the main purpose to provide and design the application to improve the measure of maritime security for ports and ships while the ISM Code provides the application to enhance the maritime safety of navigation of ships (Mukherjee, 2007). At the same time, the ISPS Code regime has the main objective to initiate an international cooperation framework among contracting governments, government agencies, local administrations and the shipping and port industry to detect, access security threats and take preventive measures against security threats to port facilities and ships involved in international trade. Second, the ISPS Code establishes the roles and responsibilities pertaining to maritime security of all concerned parties at the international and national levels to ensure efficient collation and exchange of information among concerned parties. Thirdly, the code provides a methodology for security assessments as a plan and procedure for reacting to the security level change in port facilities and ship; and lastly, ensures that adequate and appropriate maritime security measures are in place for port facility and ship (Ng & Vaggelas, 2012). In order to achieve this purpose and objective, contract governments, and port and ship operators are defined as concerned parties and provided international obligations to take measures to protect from the risk of threats to maritime security (MSC 89/INF.13, 2011).

3.1. Contracting government obligation

Contracting governments have two main international obligations to protect against threats to maritime security. The first obligation is for the maritime administration to set security levels for ships flying their national flags and to update security information
related to those ships. The second obligation of contracting government is to set up security levels for ports in the location of their territory and update information related to port facility security and ships dock at those port facilities\(^1\). Indeed, the first obligation of the contracting government as a flag state relates to regulation 3 of Chapter XI of SOLAS, which is similar to the international obligation provided by article 94 of UNCLOS 1982. In article 94 of UNCLOS, the flag state has an obligation to set a tool to provide maritime security for ships. For example, flag states shall control the administration and equipment of a ship in order to ensure safe sailing and seaworthiness. However, under the requirement of the mandatory ISPS Code part A, a flag state shall install security levels for passenger and cargo ships that only have 500 gross tonnage that relate to international trade (Mukherjee, 2007). On other hand, port facilities that have interacted with international voyages shall be affected by the ISPS Code as defined by the second obligation of contracting governments (Burmester, 2005). Beyond the main two international obligations, contracting governments also have a duty to collect information on maritime security threats related to ship and port facilities to be provided to the International Maritime Organization (IMO)\(^2\). Moreover, the security levels for ship and port facilities have three level degree differences\(^3\). Security level 1 is considered as the normal situation of commercial and trade operations, and requires the minimum appropriated to protect security measures at all times. Security Level 2 requires additional protective security measures for the specific period of time when the risk of vulnerability is heightened. The requirement of specific protective security measures only lasting for a limited period of time when risk of a security incident is probable or imminent is defined as the security Level 3 (Visvikis & Panayides, 2017). Furthermore, in order to ensure that port facilities have security levels that can protect and detect threats, the Port needs to

\(^1\) Regulation 3 of Chapter XI-2 of SOLAS
\(^2\) Section 1.6 of Part B, ISPS Code
\(^3\) Section 2.1. Part A, ISPS Code
have a Port Facility Security Plan (PFSP) and Port Facility Security Assessment (PFSA). In this sense, contracting governments will undertake PFSP and PFAS by themselves or delegate authority to a recognized security organization to do it instead of them. However, the recognized security organization can design and update the PFSP and PFSA, but the PFSP and PFSA shall be approved by the Contracting Government or Designated Authority (Visvikis & Panayides, 2017).

3.2. Ship operator responsibility

To comply with international obligations, ships need to have security to protect against terrorist attacks that may use the ship as a weapon or transport people to cause threats. In this sense, shipping companies shall appoint a Company Security Officer (CSO) on board to deal with the Ship Security Assessment (SSA) and a Ship Security Officer (SSO) on board to inspect and properly secure the ship. Furthermore, Shipping companies are required to have a Ship Security Plan (SSP) for every ship. Referring to ship security, ships need to have three levels of security that consist of security level 1, which is the suitable preventive measure against any unlawful activities that may cause threats to the security of the ship. The suitable preventive measure of Ship security level 1 is to undertake performance of ship security duties such as controlling access to the ship and the activity of people around the ship that may cause a security threat to the ship. Moreover, monitoring the restricted area and deck area around the ship in order to guarantee that only authorized persons can enter is also an element of the suitable preventive measures of ship security level 1. Moreover, ship security level 1 also takes account of the cargo handling and ship store that shall be supervised in order to prevent a

---

4 Section 4.3 Part, ISPS Code.
5 Regulation 4 of the chapter XI of SOLAS
6 Section 8.1 of ISPS Code Part A
security threat. Lastly, in case of a security threat happening, communication among relevant parties shall be available. For security level 2, ship security shall put additional protective measures on the activities of security level 1. For security level 3, ship security shall put further specific protective measures on the activities of security level 1 according to the mandatory section 7 to 7.4. of part A of the ISPS Code.

3.2.1. Ship security assessment
As stated in the mandatory section 8 to 8.4. of part A of ISPS Code, Ship Security Assessment (SSA) is an integration on the ship security history for developing and updating the Ship Security Plan. The Ship Security Assessment is done by a Company Security Officer who has appropriated professionals to evaluate ship security. The Ship Security Assessment shall identify the existent security measures, procedures and operation of the ship, and identify potential threats to the shipboard operation. The Ship Security Assessment shall focus on the weaknesses in the human factor, infrastructure, policy and procedures of the ship. Besides identifying and evaluating threats to ship, The Company Security officer also collects important information related to the assessment of the threat to the port where the ship will be docked and operation\(^7\).

3.2.2. Ship Security Plan
The Ship Security Plan is a plan for ensuring that person, cargo, and cargo transport units on board are protect from any threats of maritime security incidents\(^8\). The Ship Security Plan is prepared by the recognized security organization and approved by the administration (IMO, 2002). Indeed, as stated in section 9.4 of part A of the ISPS Code,

---

\(^7\) Section 8.2. of non-mandatory Part B of ISPS Code.

\(^8\) Section 2.1 of Mandatory Part A of ISPS Code
the Ship Security Plan shall be written in English, French and Spanish and address at least measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports. The Ship Security Plan shall be raised about the restricted areas to be prevent unauthorized persons from accessing those areas and also raised about the unauthorized person to enter the ship. Moreover, the Ship Security Plan should take account of the procedure for responding to security threats or breaches of security. At the same time, The Ship Security Plan is including provisions for maintaining critical operation of the ship, or ship and port interface procedures for evaluation in case of security threats or breach of security. Duties of shipboard personnel shall be assigned and put in the Ship Security Plan to respond to the security threat. Furthermore, The Ship Security Plan shall raise about procedure for auditing the security activity, for training, drills and exercises associated with the plan, procedure for interfacing with port facility security activities, procedure for the period of review and update plan and procedure for reporting security incidents. Lastly, the Ship Security Plan shall indicate the ship security officer and company security officer and their procedure for inspection, testing and maintenance of security equipment on board. The Ship security plan also raises about the location of the ship security alert system and instructions on use of the ship security alert system, including the testing, activation, deactivation and resetting of the system and limiting false alerts.

3.2.3. Company Security Officer

As stated in section 11 of part A of the ISPS Code, a Company Security Officer is designated to each ship and shall provide advice on threats that the ship may be vulnerable to and make suitable security assessments. Furthermore, the Company Security Officers shall make sure that the ship security assessment is undertaken submitted for approval. At the same time, the Company Security Officer also shall be sure that the Ship Security Plan is maintained and implemented. In case the ship security plan is not modified to the safety and security of each ship, the Company Security officer has the right to change and adapt
it to be satisfied. The Company Security Officer also has a duty to manage the internal audits and check the security activities. However, the Administration or recognized security organizations will arrange the initial and verification of the ship. Moreover, in case the auditor finds non-compliance during the audit, periodic review or security inspection, the Company Security officer shall respond promptly to the reason for that non-compliance. In addition, the Company Security officer shall be sure that training of the personnel for the security of the ship is fulfilled. Lastly, the Company Security Officers shall be sure that communication and cooperation between the ship security officer and port facility security officer are effective.

3.2.4. Ship Security Officer

As stated in section 12 of part A of the ISPS Code, Ship Security officers shall be designated to each ship that interacts with international voyages and has a capacity above 500 gross tonnage. In this sense, a Ship Security officer has a duty and responsibility while working on board to undertake regular security inspections of the ship and ensure that appropriate security measures are maintained, and supervise the implementation of the ship security plan. The Ship Security Officer shall coordinate with port facility security officers to ensure that cargo handling operations between the ship and port terminal and ship store are secure. Furthermore, the Ship Security Officer can also propose amendments to ship security plans. However, if non-compliance is found during an audit, review or inspection of the ship security, the Ship Security Officer shall report that non-compliance to the Company Security Officer. Moreover, Ship Security Officers also ensure that ship security training for personnel is carried out and properly report all ship security incidents. Lastly, Ship Security Officers shall cooperate with Company Security Officers and relevant Port Facility Security Officers to implement the Ship Security Plan.
2.3. **Port facilities operator responsibility**

In order to enhance maritime security, port facilities are required to have Port Facility Security Assessments (PFSA) and Port Facility Security Plans (PFSP) according to regulation 10 of SOLAS chapter XI-2. Furthermore, as stated in article 14 of part A of the ISPS Code, the Port facility is required to have three security levels based on the design by the contract government. In this sense, the security levels will be set by taking into account the appropriate measures at the port facility against security threats. The activities consist of ensuring the performance of all port facility security duties, controlling access to the port facility, monitoring of the port facility including anchoring and berthing areas, monitoring restricted areas to ensure that only authorized persons have access, supervising the handling of cargo, supervising the handling of ship’s store; and ensuring that security communication is readily available. For security level 2, additional protective measures will be added to the activities of security level 1; and for security level 3, further protective measures will be added to the activities of the security level 1.

3.3.1. **Port Facility Security Assessment**

Port Facility Security Assessment is an integration for developing and updating the Port Facility Security Plan. The contracting government shall carry out the Port Facilities Security Plan for the port facility that is located within their territory. The contracting government can delegate recognized security organizations to do the PFSA but the contracting government does review and approval on PFSAs that were carried out by recognized security organizations according to Section 15 of part A ISPS Code. Moreover, as stated in Section 15.5-part A of ISPS Code, Port Facilities Security Assessment shall be done by taking account of identification and evaluation of important assets and infrastructures that need to be protected from security threats. The Port Facilities Security Assessment also raises about the possible security threat to assets and infrastructure of the port. Lastly, the Port Facility Security Assessment shall prioritize countermeasures to the
security threats in order to reduce vulnerability to threats; and also identify the weaknesses of human element, infrastructure, policy and procedures that relate to maritime security threats.

### 3.3.2. Port Facility Security Plan

The Port Facility Security Plan is a plan that is developed and maintained on the basis of the Port Facility Security Assessment to ensure that the applicable measures are designed to protect port facility, ship, person, cargo, cargo transport units and ship dock within the port facility from the risk of a security incident according to Section 2.1. & 16.1. Part A of ISPS Code. A Recognized Security Organization can carry out the PFSP for a specific port facility but the contracting government or designated authority approves the Port Facility Security Plan (PFSP) as stated in Section 16.2 Part A of ISPS Code. The Port Facility Security Plan shall address measures designed to prevent weapons or dangerous substances and devices intended for use against port facility, ship and persons who are working in a port or ship. The Port Facility Security Plan also raises about prevention of unauthorized access to the port facility and ship and restricted area of the port facility. Moreover, PFSP shall raise on:

- The procedure for responding to security threats or breaches of security including provisions for maintaining critical operations between port facility, or port and ship interface,
- The procedure for responding to security instructions of the contracting government where the port facility is required to have security level 3
- Procedure for evaluation in case of security threats or breaches of security
- Duty of port facility personnel
- Procedure for interface with ship security
- Procedure for the periodic update and review of PFSP
- Procedure for reporting on security incidents
- Measures to ensure the security of the information existing in the PFSP
- Measures to ensure that cargo and cargo handling equipment have effective security
- Procedure for auditing the PFSO
- Procedure for responding in case of security alert from ship at the port facility
- Procedure for facilitating shore leave for ship’s personnel or personnel change, or visitor access to ship, which includes seafarer welfare and labor organizations.

3.4. Summary

The ISPS Code regime has set international obligations for ships and ports involved in international trade to set security levels to prevent and detect any threats to maritime security. Firstly, port facilities involved in international trade shall set a Port Facility Security Plan that is improved and updated based on the Port Facility Security Assessment. Secondly, passenger ships and cargo ships of 500 gross tonnage and upward that engage in international voyages shall set a Ship Security Plan which is developed and updated based on the Ship Security Assessment.
Chapter 4

National obligations related to maritime security derived from national law of Cambodia

A legal framework and maritime administration are necessary for contracting governments to implement the ISPS Code because maritime administrations or designated authorities are required to set security for ports and ships instead of contracting government as stated in regulation 3 of Chapter XI-2 of SOLAS. Moreover, the legal framework is also important to set an obligation for all participants within a contracting state to respond to maritime security. The participants involved in maritime security are the port and shipping industries because those participants are vulnerable to maritime security threats such piracy and armed robbery (UNCLOS, 1982) and maritime terrorism (Mensah, 2004). Therefore, this chapter will analyze the national obligations set by the national law of Cambodia pertaining to maritime security for port and ship operators.

4.1. Legal Framework.

Cambodia participated in implementing the ISPS code, which is part of SOLAS, in order to protect against and mitigate risks in the maritime transport sector. In this sense, Cambodia has adopted its own national regulation framework to comply with the ISPS Code. The Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security was adopted on May 09, 2006. The Sub-Decree # 40 (RGC) has the main objective to control the ship and port facility security of the Kingdom of Cambodia through international cooperation with other contracting governments, shipping companies, and ports involved in sea-going transport. However, this regulation is not running well until the Prakas No 432 BK on the port facilities of Cambodia in order to implement Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security that was adopted on May 09, 2006 was adopted on December 20th 2017 by the Ministry of Public Work and Transport (MPWT).
The Prakas No 432 BK has the main objective to control port facility security in Cambodia.

**Legal Framework**

SOLAS-ISPS Code

Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security in 2006

Prakas No 432 BK on the port facilities of Cambodia in 2017

Table 2: Legal framework of Cambodia relate to Maritime security

### 4.2. Maritime administration

Maritime administration carries out the main role of management, control, facilitation and implementation of policy on behalf of the state to comply with international regulations involving the maritime sector (Mukherjee & Brownrigg, 2013). For instance, as stated in article 41 of the Prakas No 432 BK, the General Department of Waterway and Maritime Transport, and Port of the Ministry of Public Work and Transport (MPWT) is the maritime administration of Cambodia. It checks the activities of all foreign ships that enter into Cambodian ports and all relevant authorities such as customs and immigration that are related to port facility security. The General Department of Waterway and Maritime Transport, and Port coordinates communication between the Ministry of Public Works and Transport (MPWT) and the International Maritime Organization. Moreover, within the article 46 of the Prakas No 432 BK, the General Department of Waterway and Maritime Transport and Port has the main task to provide information to the International Maritime Organization on national regulations to implement the ISPS Code, address and
name of recognized security organization, port facility security assessment and list of port facilities security plan within a 5-year period. Furthermore, according to article 4 of Prakas No 432 BK, the General Department of Waterway and Maritime Transport and Port prepare and check the qualifications of recognized security organizations to implement the task of port security assessment, port facility security plan, check and revise port facility security plan, and provide advice and recommendations on port security assessment and port facilities security plan. The recognized security organization will be under the hand of the General Department of Waterway and Maritime Transport, and Port. Furthermore, it is good that article 5 of Prakas No 432 BK addresses that the recognized security organization will be not allowed to advice and recommend on the port facility security plan which was done by themselves. At the same time, the recognized security organization also not allow to advice and recommend on the port facility security assessment which was done by themselves. In this sense, the General Department of Waterway and Maritime Transport and Port has the right to audit and investigate the recommendation on port facility security assessment and port facility security plans that were done by recognized security organizations. Therefore, if the General Department of Waterway and Maritime Transport and Port finds the recommendation on the port facility security assessment and port facility security plan done by the same recognized security organization, those recommendations on PFSA and PFSP will be rejected.
4.3. Recognized Security Organization

As stated in articles 3 and 6 of Prakas No 432 BK on the port facilities of Cambodia, in order to implement the Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security on December 20th 2017, a Recognized Security Organization was selected by the General Department of Waterway and Maritime Transport and Port and nominated by the Ministry of Public Work and Transport. In this sense, The General Department of Waterway and Maritime Transport and Port select Recognized Security Organization by taking an accountable to their professional on the port facility security risk management, knowledge of ship and port operation, knowledge of the port layout and port
infrastructure, and capacity of assessment of risk vulnerability in the operation between
ship and port. Furthermore, the Recognized Security Organization has the capacity to
reduce and minimize the risks of maintenance and development of the skills of their staff.
In addition, the Recognized Security Organization shall have the ability to keep and store
important documents related to port security and knowledge on the international and
national law related to security. Knowledge of current security threat characteristics and
analysis of the weapon research are necessary for the Recognized Security Organization.
The Recognized Security Organization needs to have knowledge about hazard substances
and equipment and identification of people that may cause risks to port security.
Moreover, the Recognized Security Organization shall have knowledge of plans to prevent
attacks on port security and knowledge of security tools and systems, as well as the level
of use of those tools and systems. After nomination, the Recognized Security Organization
has the duty to carry out the PFSA and PFSP. However, as stated in article 5 of Prakas No
432 BK, the Recognized Security Organization who does Port Facility Security
Assessment will not be allowed to provide advice and recommendation on Port Facility
Security Assessment while the Recognized Security Organization who design port
security plan will not be allowed to provide advice and recommendation on Port Facility
Security Plan. Moreover, the Recognized Security Organization who does port facility
security assessment will not be allowed to designate a Port Facility Security Plan at the
same port.
Recognized Security Organization (Article 4 & 6 of Prakas No 432 BK)

Step 1: Selected by General Department of Waterway and Maritime Transport, and Port

Step 2: Nominated by Minister of Public Work and Transport

Duty of Recognized Security Organization:
- Carry out Port Facility Security Assessment
- Carry out Port Facility Security Plan
- Except the approval on PFSA & PFSP

Table 3: Recognize Security Organization

4.4. National Obligation of Port Facility Operator

According to article 35 of the Sub-Decree # 40 (RGC), a port facility is required to set security levels that consist of three levels. Security level one shall be installed in order to identify and take preventive measures against security incidents that ensure the performance of all port facility security duties. Furthermore, Security Level 1 would be installed in order to control access to the port facilities, and monitor of the port facility, including anchoring and bathing areas; and monitor restricted areas to ensure that only authorized persons have access. Security Level 1 also involves the supervision of cargo handling, supervision of the ship's tours and ensuring that security communication is readily available. For security level 2, the port facility shall set additional protective and security measures in order to strengthen security level 1. For the security level three, the port facility shall set further specific protective measures to mitigate and protect any incident happening. In this sense, applying to port facility security, Cambodia has 7 sea ports and 42 rivers ports but among them there are only two main ports that interact with international trade. Those ports are Sihanoukville Autonomous Port (PAS) which is the
sea port and the other is Phnom Penh Autonomous Port (PAP) which is a river port. Both are considered as the international ports of Cambodia (JICA-Part 2, 2017). Consequently, as stated in the article 7 of the Sub-Decree # 40 (RGC), the Sihanoukville Autonomous Port (SAP) and Phnom Penh Autonomous Port (PAP) or other International Ports of the Kingdom of Cambodia shall be defined by the Royal Government to comply with the Sub-Decree # 40 (RGC) to have port facility security as mentioned in the article 35 of the Sub-Decree # 40 (RGC).

4.4.1. Port facility Security Assessment

As stated in articles 10 to 12 of Prakas No 432 BK, PFSA shall be addressed on three main aspects that consist of physical, vulnerability of threat and vulnerability of source of risk. First, for the physical aspect of the port facility are identified by considered to port security officers, integrity of construction and building, protection system for employees working in the port, work procedure, telecommunication and computer system, transportation infrastructure, electrical equipment and areas that may pose risks to people, property and operations in the port. Second, the vulnerability of threat includes:

- Any possible loss or damage to the property of the port facility or ship which is docking in the birth of the terminal by use of explosives, theft, shock and other violence,
- Shipwreck or hijacking or hijacking of people on board,
- Smuggling of national weapons, and explosive equipment, including weapons of mass destruction
- Unauthorized access into the vessel while docking at the port
- Use of ships to transport people and equipment intended to cause security incidents
- Using the ship as a weapon, as a means of causing damage or destruction
- Blocking or closing the entrances of port facilities
- Nuclear, biological and chemical weapons attacks
- And other security threats.
Third, the vulnerability of risk sources is identified in the waterway and land access to the port facility and ships that dock in the ports that can cause threats. The vulnerability of risk sources also reviews the existing security measures and procedures that include identification systems, security measures and procedures related to port services and electrical equipment because these factors can be sensitive to the port facility threats. In addition, the measures to protect radio and telecommunication equipment are defined as necessary to prevent any vulnerability risks to the port facility. Furthermore, the vulnerability of risk sources takes into account port services, electrical equipment and neighboring areas that can be used to attack or for the purpose attacking of the port facility. Existing agreement with private security companies that provide security services at waterway and land entrances are necessary to check and control in order to make effective measures to prevent vulnerable risk. Furthermore, the consistent barriers to law enforcement and lack of human resources are classified as vulnerability risks to port security. Lastly, reports of port security issues, security announcements and security internal audits play a central role in following up the vulnerable risk threat to port facility.

**Port Facility Security Assessment (article 10, 11 & 12 of Prakas No 432 BK)**

**General Department of Waterway and Maritime Transport, and Port**

- Approval on the PFSA

- Reorganize Security organization

  - Do PFSA by identify and analysis on the main three aspects that consist of (1). physicality, (2). vulnerability of threat and (3). vulnerability of source of risk.

Table 4: Port Facility Security Assessment
4.4.2. Port Facility Security Plan

As stated in articles 13, 14 & 15 of Prakas No 432 BK, Port Facility Security Plan shall be focused on four aspects, namely information security, infrastructure of port facility, people and procedure of working and operation; and security levels for any threats or attacks. Firstly, for information security of the port, PFSP shall:

- Provide detailed information on the port facility governance structure
- Provide detailed information on the connection structure between the port and relevant authorities to effectively implement the security measures
- Provide detail information on security level 1
- Provide additional detailed information that can allow port facility operators continue to implement security level 2 and level 3 without any time delay.
- Recheck and auditing regularly on the PFSP or amendment to PFSP
- Provide detailed information on the process of making a report to the General Department of Waterway and Maritime Transport, and the Port of Ministry of Public Work and Transport.

Secondly, the port facility infrastructure shall be defined in the PFSP. Indeed, Port Facility infrastructure refers to container terminal, cruise terminal, service passenger, RO-RO service terminals, commuter and vehicle, liquid bulk terminal, gas terminal, dry bulk terminal and multi modal terminal where the ship and port interact with each other, such as at anchorage, and awaiting berths and approaches from seaward (Andritsos, 2013). Thirdly, people and procedures of working shall be defined in the PFSP and may include:

- Role and duties of port facility security officer
- Connection structure between port facilities security officer and other security authorities
- Connection system between port facilities security officers and other security authorities
- Procedures that ensure daily connections happen all the time
• Procedures to protect important security information that has been stored in written or electronic form.

• Procedure of evaluation of the effectiveness of security measures, security procedures, and security equipment, including identification, responding and device malfunction

• Procedure of reporting security violations and security issues

• Procedure of loading and unloading cargoes

• Procedures related to the delivery of goods

• Procedures related to the delivery of ship

• Procedures to maintain correct records of goods, hazardous substances and the places where the goods are located

• Emergency warning and maritime patrol services and specialized inspections, including underwater explosives research

• Procedures to assist the ship’s security officer in verifying the identity persons who seeking to board the ship

• Procedures for facilitating crew landings or for crew changes as well as the entry of tourists to the ship, including representatives of the crew.

Lastly, the Port Facility Security Plan shall be installed the three security levels at the access road to the port facilities, prohibited areas in the port facilities, loading and unloading goods, delivery of goods, delivery of ship and guard on the port facility security.
Port Facility Security Plan (Article 13, 14 & 15 of Prakas No 432 BK)

Shall consist of:

1. information security,
2. infrastructure of port facility,
3. people and procedure of working and operation;
4. and security levels for any threats or attacks.

Table 5: Port Facility Security Plan

4.5. National Obligation of Ship Operator

As stated in articles 4 and 27 of the Sub-Decree # 40 (RGC), a Cambodian Passenger and Cargo Ship that has more than 500 gross tonnage and interacts with international trade shall set security that consists of three levels and has Ship Security Assessment and Ship Security Plan. According to article 26 of the Sub-Decree # 40 (RGC), the Ship Security Level 1 shall identify and take preventive measures to protect any threat to the ship by implementing ship security, controlling access to ship, checking persons who stay on board the ship and their personnel items, guarding the restricted area, monitoring all ship decks and its surrounding, inspecting handling, maintenance and transfer of cargo; and ensuring that communication of security is available. Furthermore, Ship Security Level 2 is an additional preventive measure to ship security level 1. Lastly, Ship Security Level 3 is further preventive measure on the ship security level 1 in order to protect and detect any threats to the ship.

4.5.1. Ship Security Assessment

The Cambodia ship register committee delegates authority to the Recognized Security Organization to carry out the Ship Security Assessment according to article 10 of Sub-Decree # 40 (RGC). As stated in article 29 of Sub-Decree # 40 (RGC), a Recognized
Security Organization carries out the Ship Security Assessment by taking on-site on
security surveys and reporting on key factors including:

- Identification of existing security measures, procedures and operations
- Identification and evaluation of key operations on ships that need to be
  protected
- Identification of potential threats to ship operations
- Identification of weaknesses, including human factors in infrastructure,
  policies and procedures

4.5.2. Ship Security Plan

As stated in article 10 of Sub-Decree # 40 (RGC), a Recognized Security Organization
carries out a ship security plan. Ship Security plan should be designed based on the ship
security assessment according to article 30 of Sub-Decree # 40 (RGC).

4.6. Summary

Port facilities involved in international trade are required to have Port Facility Security
Assessments and Port Facility Security Plans according to the requirements of Sub-Decree
# 40 (RGC) on Vessel Security and Port Facility Security on May 09, 2006 and Prakas No
432 BK on the port facilities of Cambodia in order to implement Sub-Decree # 40 (RGC)
on Vessel Security and Port Facility Security on December 20th 2017. While ships that
fly the flag of Cambodia of at least 500 gross tonnage and sailing on international voyages
shall be set security levels in the Ship Security Plan that was updated based on the Ship
Security Assessment as the requirement of Sub-Decree # 40 (RGC) and Prakas No 432
BK.
Chapter 5

Legal Analysis between international obligations and national obligations relates to maritime security

The ISPS Code is the international legal framework to provide contracting states, ports and the shipping sector with duties to protect and prevent threats to maritime security (Mensah, 2004). Cambodia is a contracting party to the ISPS Code and as a contracting government, Cambodia has a duty to prevent threats and protect maritime security. Therefore, The Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security was adopted on May 09, 2006 and the Prakas No 432 BK on the port facilities of Cambodia was adopted on December 20th 2017 for the legal framework of Cambodia to enhance maritime security. This chapter will focus on a legal analysis between obligations related to maritime security at the international level and national level of Cambodia to determine whether those obligations are harmonized or conflict with each other. Furthermore, this chapter also undertakes a legal analysis to determine which part of the national obligations of Cambodia in compliance with international obligation related to maritime security are available to implement and which are difficult to implement. In order to see the harmonization or conflict between international and national obligations relates to maritime security, therefore, regulations of the ISPS Code, Sub-Decree # 40 (RGC) and the Prakas No 432 BK related to port facility security, port facility security assessment, port facility security plan, ship security, ship security assessment and ship security plan will be analyzed.

5.1. Harmonization

Firstly, section 3 of part A of the ISPS Code and article 2 of The Sub-Decree # 40 (RGC) on the effective implementation of ship and port are harmonized with each other. For example, both articles state that ports involved with international trade and passenger and
cargo ships that have 500 gross tonnage or above will apply maritime security measures that consists of port facility security and ship security.

Second, section 7 of part A ISPS Code and article 26 of The Sub-Decree # 40 (RGC) on ship security are in harmony with each other because both articles address security level 1 to level three on a ship in the same way. For example, in terms of security level, both articles address seven aspect of preventive security measures that consist of ensuring performance of all ship security duties, controlling access to the ship, controlling the embarkation of persons and their personal items, monitoring restricted areas to ensure that only authorized persons have access, monitoring of deck areas and areas surrounding the ship, supervising the handling of cargo and ship’s store ; and ensuring that security communication is ready available.

Thirdly, section 8 of part A ISPS Code and article 29 of The Sub-Decree # 40 (RGC) on the ship security assessment are in harmony with each other because both articles treat security assessment of ships in the same way. For instance, both articles address on scene security surveys based on four keys points that consist of the identification of existing security measures, procedures and operations, identification and evaluation of key onboard operations that are of importance to protect, identification of possible threats to the key onboard operations and the likelihood of their occurrence in order to establish and prioritize security measures, identification of weaknesses including human factors, infrastructures, policy and procedure.

Fourthly, section 14 of part A ISPS Code and article 35 of The Sub-Decree # 40 (RGC) on port facility security are harmonized because both articles address security of port facilities in the same way, from port facility security level 1 to security level 3. For example, regarding security level 1 of port facilities, both articles address seven aspects that consist of ensuring the performance of all port facility security duties, controlling access to the port facility, monitoring of the port facility including anchoring and berthing.
areas, monitoring restricted areas to ensure that only authorized persons have access, supervising the handling of cargo, supervising the handling of ship’s store; and ensuring that security communication is ready available.

Fifth, section 15 of part A ISPS Code and article 10 of the Prakas No 432 BK on port facility security assessment are in harmony because both articles address PFSA in the same way. For instance, Port facility security assessment shall identify and evaluate important assets and infrastructure that need to be protected, identify the possible threats to the assets and infrastructure, identify, select and prioritize countermeasures and, procedures in order to reduce vulnerability, and identify weakness including human factors, infrastructure, policy and procedure.

Sixth, section 16 of part A ISPS Code and article 13, 14 & 15 of the Prakas No 432 BK on port facility security plan are harmonized because those articles have the same meaning. For example, section 16 of part A ISPS Code addresses measure to restrict weapons and dangerous substances, and prevent unauthorized access to the port facility and ship, while article 15 of the Prakas No 432 BK address security levels that need to be installed in the access road to the port facilities, prohibited areas in the port facilities, loading and unloading goods, delivery of goods, delivery of ship and guard on the port facility security.

5.2. Conflict

The content of the national law of Cambodia involving maritime security is not on conflict or different in meaning from the content of the ISPS Code because the national law of Cambodia that relates to maritime security has been modeled on the content of the ISPS Code. For instance, the content of the port facility security plan and port facility security assessment are harmonized. Furthermore, the content of the Ship Security Assessment and Ship Security Plan are also harmonized.
5.3. Available for Implementation

New national obligations related to maritime security that derive from Cambodian regulation started implementation in 2006. Port facility and ship security in the new obligations relate to requirements of The Sub-Decree # 40 (RGC) & the Prakas No 432 BK. At the same time, some content of The Sub-Decree # 40 (RGC) & the Prakas No 432 BK has been implemented. For example, article 35 of The Sub-Decree # 40 (RGC) and article 13, 14 & 15 of the Prakas No 432 BK has been implemented by Phnom Penh Autonomous Port via creating its port facility security plan. For instance, in July 2019, Phnom Penh Autonomous Port published its PFSP for Phnom Penh New Container Terminal LM17 in the period of five years in order to comply with the Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security that was adopted on May 09, 2006, Prakas No 432 BK on the port facilities of Cambodia on December 20th 2017 and the Chapter XII of the International Convention on the Safety of Life at Sea (SOLAS) and Part A of the International Ships and Ports Facility Security (ISPS) Code. The PFSP for Phnom Penh New Container Terminal LM17 has the main objective to promote security and safety of human life, ship, cargoes and port facility in order to improve international commercial cooperation between the Phnom Penh New Container Terminal LM17, shipping companies and other international ports; and suppress all export and import of contraband, theft and terrorism activity which may sabotage the port facility and ship. PFSP of Phnom Penh New Container Terminal LM17 mainly focuses on six areas that consist of (1) the location of port facilities and (2) Defining the port facilities infrastructure (3) port facility security measures (4) installation and maintenance of port facilities security (5) Designating a port facility security officer and their duties, training, drilling and exercises on port facility (6) and responding to security hazard incidents (PFSP of PPAP, 2019).
5.4. Difficult to Implement

Indeed, the content of the Port Facility Security, Port Facility Security Assessment and Port Facility Security Plan has been implemented by Phnom Penh Autonomous Port. However, the Port Facility Security Plan was done by Phnom Penh Autonomous Port itself, which is opposite to the intention of article 4 of Prakas No 432 BK which states that a Recognized Security Organization delegated by the General Department of Waterway and Maritime Transport, and Port will carry out the Port Facility Security Plan and Port Facility Assessment (PFSP of Phnom Penh Autonomous Port, 2019). Furthermore, after being carried out by the Recognized Security Organization, the Port Facility Security Plan shall be approved by the General Department of Waterway and Maritime Transport, and Port according to article 4 of Prakas No 432 BK. At the same time, Section 16.1.1 and 16.2 Part A of ISPS Code also states that the Port Facility Security Plan may be carried out by a Recognized Security Organization and approved by the Contracting Government. In this sense, the Port Facility Security Plan of Phnom Penh Autonomous Port shall be carried out by a Recognized Security Organization. Consequently, it may be difficult to find a Recognized Security Organization in Cambodia who has enough capacity according to the requirements of article of articles 3 and 6 of Prakas No 432 BK on the port facilities of Cambodia in order to implement Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security on December 20th 2017, which requires a Recognized Security Organization that has at least a professional on port facility security risk management, knowledge of ship and port operation, knowledge on the port layout and port infrastructure, capacity of assessment on risk vulnerability in the operation between ship and port. Therefore, article 4 of Prakas No 432 BK would be difficult to implement.

Furthermore, article 2.2. of The Sub-Decree # 40 (RGC) requires that ports that interact with ships that have 500 gross tonnage and are engaged in international voyages shall have Port Facility Security Plans and Port Facility Security Assessments. At the same time, article 7 of the Sub-Decree # 40 (RGC) claimed that only the Sihanoukville Autonomous
Port (SAP) and Phnom Penh Autonomous Port (PAP) or other International Ports of the Kingdom of Cambodia shall be defined by the Royal Government to comply with the Sub-Decree # 40 (RGC) to have port facility security as mentioned in the article 35 of the Sub-Decree # 40 (RGC). In fact, Cambodia has 7 sea ports and 42 river ports. Among 7 sea ports, there are 3 private ports that also interact with international trade such as Sre Ambel Port, Oknha Mong Port and Oil Terminal (JICA-Part 2, 2017). In this sense, the three private sea ports shall have Port Facilities Security Plan and Port Facility Security Assessment according to article 2.2. Of the Sub-Decree # 40 (RGC). Therefore, article 2.2. Of the Sub-Decree # 40 (RGC) seems not yet in full implementation because the three private sea ports do not yet have a Port Facilities Security Plan and Port Facility Security Assessment.

5.5. Summary

National obligations related to maritime security derived from the national law of Cambodia are in harmony with international obligations related to maritime security derived from the ISPS Code. However, there is still a lack of full implementation of some articles, such as article 4 of Prakas No 432 BK on the Recognized Security Organization and article 2.2. Of the Sub-Decree # 40 (RGC) Port Facility Security Plan and Port Facility Security Assessment for ports that interact with international trade.
Chapter 6

6.1. Conclusion

The ISPS Code Regime has provided for contracting governments international obligations to set up security levels in their ports that interact with international trade and ships engaged in international voyages of 500 gross tonnage and above. Port and Ship facilities have three security levels that need to be installed. Security level 1 is considered as the normal situation of commercial and trade operations, and requires the minimum appropriated to protect security measures at all times. Security Level 2 requires additional protective security measures for the specific period of time when the risk of a security incident is heightened. The requirement of specific security measures for only a limited period of time when a security incident is probable or imminent is defined as security Level 3 (Visvikis & Panayides, 2017). Furthermore, ports shall have Port Facility Security Plans and Port Facility Security Assessments, while ships shall have Ship Security Plans and Ship Security Assessments. At the same time, Cambodia, as a contract government to the ISPS Code, needs to comply with the requirements of ISPS Code in terms of maritime security. Therefore, the Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security was adopted by May 09, 2006 and the Prakas No 432 BK on the port facilities of Cambodia was adopted on December 20th 2017 as the legal framework of Cambodia to set the national obligations for Port Operators and Ship Operators. Indeed, as stated in the Sub-Decree # 40 (RGC), ports located in Cambodia’s territorial waters and interacting with international trade and passenger and cargo ships that have at least 500 gross tonnage will be subject of maritime security measures that consist of port facility security and ship security. Moreover, as stated in article 41 of the Prakas No 432 BK, the General Department of Waterway and Maritime Transport and Port under the provision of the Ministry of Public Work and Transport shall set the security levels that consist of three levels for port and ship operators in application of maritime security measures to detect
and protect any port and ship facility from maritime security threats. Therefore, the national obligations related to maritime security of Cambodia are harmonized with international obligations derived from the ISPS Code. However, the implementation of national obligations related to the Port Facility Security Plan are not yet in full effect for all ports of Cambodia that interact with international trade. For example, there are only two state owned ports that consist of Phnom Penh Autonomous Port and Sihanouk Autonomous Port that apply the national obligations related to maritime security. However, three private ports, namely Sre Ambel Port, Oknha Mong Port and Oil Terminal that also interact with international trade are not yet in compliance with the requirements of national obligations related to maritime security (JICA-Part 2, 2017). Furthermore, it also seen that Port the Facility Security Plan shall be carried out by a Recognized Security Organization, according to according to article 4 of Prakas No 432 BK. Nevertheless, the Port Facility Security Plan is done by the port itself. For example, the Port Facility Security Plan of Phnom Penh Autonomous Port in 2019 was done by Phnom Penh Autonomous Port itself (PFSP of Phnom Penh Autonomous Port, 2019).

6.2. Recommendations

1. The Port Facility Security Plan shall be carried out by a Recognized Security Organization in order to apply with the requirements of articles 3 and 6 of Prakas No 432 BK on the port facilities of Cambodia in order to implement Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security, December 20th 2017.

2. Ports located in Cambodia’s territorial waters that interact with international trade shall install security application measures as per the requirement of article 7 of the Sub-Decree # 40 (RGC). For example, Sre Ambel Port, Oknha Mong Port and Oil Terminal shall install security in compliance with the requirement of the article 7 of the Sub-Decree # 40 (RGC) because these ports also interact with international trade.
Reference:


Prakas No 432 BK on the port facilities of Cambodia in order to implementation of the Sub-Decree # 40 (RGC) on Vessel Security and Port Facility Security


Sub-Decree # 40 (RGC) has the main objective to control the ship and port facility security of the Kingdom of Cambodia


