Maritime Supply Chain Security Gaps of Middle Powers*

Orta Güçlerin Deniz Tedarik Zinciri Güvenlik Açıkları

Oğuzhan TÜREDİ** and Hakkı KİŞİ***

Abstract

This paper aims to find out the maritime supply chain security gaps that middle powers might encounter by comparing the maritime supply chain security of the dominant power, the US, and the middle power, Turkey. To accomplish this benchmarking, the Two Axes Multi-Sector (TAMS) model that enabled the multi-layered based security analysis throughout the two flows -cargo flow and transit flow- running in the logistics channel is introduced. As a result of the comparison with the TAMS model, the maritime supply chain security gaps of the middle powers can be divided into three distinct categories. First group of security gaps need the efforts of the international organizations to be overcome. Second group of security gaps need grants and funds from the dominant power or international organizations to be overcome. Third group of security gaps need the middle power vision regarding maritime supply chain security.

* This paper is achieved as a result of a research engaged the Ph.D. thesis carried out at the California Maritime Academy of the United States in 2012, which was sponsored by the Turkish General Staff and the Turkish Coast Guard and funded by the Scientific and Technological Research Council of Turkey (TÜBİTAK). Special thanks go to Dr. Donna J. Nincic, the research supervisor, at the California Maritime Academy.

** Ph.D. Candidate, Dokuz Eylül University, Maritime Faculty, e-mail: oguzhan.turedi@ogr.deu.edu.tr.

*** Prof. Ph.D., Dokuz Eylül University, Maritime Faculty, Department of Marine Transportation Engineering, e-mail: hakki.kisi@deu.edu.tr.

Keywords: *SCS (Supply Chain Security), security initiatives, TAMS (Two Axes Multi-Sector) model, logistics channel, middle powers.*

Öz

Bu makalenin amacı, orta güç Türkiye ve dominant güç ABD'nin deniz tedarik zincirlerini karşılaştırmak suretiyle, dünyadaki orta güçlerin karşılaşabileceği deniz tedarik zinciri güvenlik açıklarını bulmaktır. Bu karşılaştırmayı yapabilmek için, yük akışı ve transit akış olmak üzere, lojistik kanaldaki iki akış boyunca çok katmanlı güvenlik analizine imkân sağlayan TAMS (İki Eksenli Çok Sektörlü) modeli geliştirilmiştir. TAMS modeli ile yapılan karşılaştırma neticesinde, orta güçlerin deniz tedarik zinciri güvenlik açıklarının üç farklı grupta toplanabilir olduğu sonucuna ulaşılmıştır. Birinci grup, kapatılması için uluslararası organizasyonların çabasına ihtiyaç duyulan güvenlik açıkları; ikinci grup, kapatılması için uluslararası organizasyonların veya dominant gücün maddi yardımına ihtiyaç duyulan güvenlik açıkları; üçüncü grup, kapatılması için orta güçlerin deniz tedarik zinciri güvenliği ile ilgili bütünleşik bir vizyona sahip olmasının gerektiği güvenlik açıkları.

Anahtar Kelimeler: *Tedarik Zinciri Güvenliği, güvenlik inisiyatifleri, TAMS (İki Eksenli Çok Sektörlü) modeli, lojistik kanal, orta güçteki ülkeler.*

1. Introduction

The "dominant nation" resides at the top of the global hierarchy in the Power Transition Theory[1] which conceptualizes world politics as a hierarchical system. "Great powers" populate the second tier of

[1] For more about Power Transition Theory, see A.F. Kenneth Organski, ***World Politics***, Knopf, New York, NY, 1968; A.F. Kenneth Organski and Jacek Kugler, ***The War Ledger***, University of Chicago Press, Chicago, IL. 1980; Douglas Lemke and Jacek Kugler, "The Evolution of the Power Transition Perspective", Jacek Kugler and Douglas Lemke, (ed.), ***Parity and War: Evolutions and Extensions of The War Ledger*** , University of Michigan Press, Ann Arbor, MI, 1996, 3-34; Ronald L.Tammen et. al. ***Power Transitions: Strategies for The 21st Century***, Chatham House, New York, NY, 2000.

international power. Beneath the great powers are the 'middle powers' and further down the power hierarchy reside the 'small powers'.

The dominant nation in this theory is not the hegemon but rather the recognized pre-eminent, most powerful international leader.[2] After September 2001 attacks, the US (United States), as a dominant power, forced the member states of International Maritime Organization (IMO) to adopt the International Ship and Port Facility Security (ISPS) Code. In stark contrast with the usual time frame of about 10 years for adaptation of such conventions, for the first time in IMO history, mandatory international measures covering the world's shipping were drafted, adopted and implemented within a span of two years.[3] The US also imposed the Container Security Initiative (CSI) and the Custom-Trade Partnership against Terrorism (C-TPAT) as the bilateral voluntary measures and enacted the Maritime Transportation Security Act (MTSA) of 2002 and imposed 96-hour advance notification of arrival, crew visa requirements, and 24-hour advance manifest rule as the unilateral measures.

Neither middle powers nor great powers would be able to force all the other states and stakeholders to adopt these measures. The US, as a dominant nation, created the status quo in maritime domain and still defends it.

On the other hand, according to the Power Transition Theory, middle powers can make serious demands that cannot be dismissed but they do not have the capabilities to challenge the dominant power for control of the global hierarchy.

Most of the middle powers cannot make maritime security policies that they need. This may be due to their insufficient resources,

[2] Jacek Kugler and Ronald L. Tammen, "Regional Challenge: China's Rise To Power", Jim Rolfe, (ed.), ***The Asia-Pacific: A Region in* Transition**, Asia-Pacific Center for Security Studies, Honolulu, HI, 2004, 33-53, p. 35.

[3] Prakash Metaparti, "Rhetoric, Rationality and Reality in Post-9/11 Maritime Security", ***Maritime Policy and Management***, 2010, Vol. 37, No. 7, 723-736, p. 726.

the resistance of the stakeholders or their non-maritime vision. For example, even in European Union (EU) which is a great power in toto[4] and comprises of middle and small powers, the general public attitude as regards to the existing, or perceived, security policy gaps seems to be a minor issue, whereas cost implications of the rule are assessed to be substantial.[5] In other words, a middle power is not a policy maker on both national and international level.

2. Factors Effecting to the Subject

2.1. United Nations (UN)-led Security Initiatives

The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), 1988: The main purpose of this convention is to ensure that appropriate action is taken against persons committing unlawful acts against ships.

International Ship and Port Facility Security (ISPS) Code: IMO introduced a new chapter XI-2 concerned maritime security to the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74) and a new Code with two parts including mandatory Part A and recommendatory Part B in 2002.

SAFE Framework of Standards: World Customs Organization (WCO) presented SAFE Framework of Standards to Secure and Facilitate Global Trade in 2005. Eventually, SAFE Framework was improved in 2007, 2010, and 2012.

The Seafarers' Identity Documents Convention (Revised), 2003: ILO revised the former 1958 convention in 2003. This convention was adopted to facilitate the entry of seafarers into the territory of members, for the purposes of shore leave, transit, transfer, or repatriation.

Code of Practice on Security in Ports: The ISPS Code

---

[4] Jacek Kugler and Ronald L. Tammen, p. 36

[5] Athanasios A. Pallis and George K. Vaggelas, "EU Port and Shipping Security", Wayne K. Talley, (ed.), ***Maritime Safety, Security and Piracy***, Informa, London, 2008, 235-255, p. 247.

requirements are related to the security of ship and to the immediate ship-port interface (port facility). On the other hand, this code of practice of 2004, which is approved by the International Labor Organization (ILO) and IMO, extends the consideration of port security beyond the area of the port facility into the whole port. It is not a legally binding instrument and is not intended to replace the ISPS code.

Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea: The Convention is adopted in 2008 and establishes a uniform and modern legal regime governing the rights and obligations of shippers, carriers and consignees under a contract for door-to-door carriage that includes an international sea leg.

2.2. US-led Security Initiatives

Customs-Trade Partnership against Terrorism (C-TPAT): C-TPAT, that began in November 2001 and codified by the SAFE Port Act of 2006, is a voluntary partnership between Customs and Border Protection (CBP) and industry to secure the international supply chain from end to end.

Advance Electronic Cargo Information (24-Hour Rule): Adopted in 2002 (in force since February 2003), this rule requires that manifest information on cargo destined for the US must be provided 24 hours prior to container being loaded onto a vessel in a foreign port.[6]

Container Security Initiative (CSI): CSI was developed by the CBP in the aftermath of 9/11 terrorist attacks (codified by SAFE Port Act of 2006) and it proposes a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at participating foreign ports before they are placed on vessels destined for the US.[7]

Megaports: Under this program, which began in 2003, the Department of Energy's National Nuclear Security Administration

[6] US Department of Homeland Security, ***Strategy to Enhance International Supply Chain Security***, 2007, p. 67.
[7] US Department of Homeland Security, ***ibid***, 2007, p. 68.

(DOE/NNSA) installs radiation detection equipment in the world's largest and busiest ports to help detect, deter, and interdict illicitly trafficked nuclear and other radioactive materials through the global maritime system before they reach the US shores.[8]

Secure Freight Initiative (SFI): SFI is initiated as a requirement of SAFE Port Act, which introduces the deployment of pilot integrated scanning system including non-intrusive inspection (NII) and radiation detection equipment at three distinct foreign ports. Major difference between the SFI and CFI is that the latter works on a reciprocal base, while the former is a unilateral.[9]

Proliferation Security Initiative (PSI): PSI, announced by President Bush on May 31, 2003, seeks to stop shipments of weapons of mass destruction (WMD), their delivery systems, and related materials to and from the States and the non-State actors worldwide.[10] The initiative gives the US the right to board and inspect ships flying the flags of the partner states on the high sea suspected of carrying VMD.[11]

International Port Security Program (IPSP): Under this program, which was established by the US Coast Guard (USCG) in April 2004, the USCG and host nations work jointly to evaluate the countries' overall compliance with the ISPS code.[12] Coast Guard officials reported that from its inception in April 2004 through June 2013, IPS program officials have visited port facilities in 151 countries and overseas

[8] US Department of Homeland Security, ***International Outreach and Coordination Strategy***, 2005a, p. B-1.
[9] Athanasios A. Pallis and George K. Vaggelas, ***ibid***, p. 238.
[10] US Department of Homeland Security, ***ibid***, 2005a, p. B-3.
[11] Chris Rahman, "Evolving U.S. Framework for Global Maritime Security from 9/11 to the 1000-ship Navy", Rupert Herbert-Burns, et. al., (ed.), ***Lloyd's MIU Handbook of Maritime Security***, CRC Press, London, 2008, 39-53, p. 43.
[12] US Department of Homeland Security, ***ibid***, 2005a, p. B-5.

protectorates engaged in maritime trade with the United States. [13]

2.3. Industry-led Security Initiatives

ISO standards: ISO has produced Publicly Available Specifications (PAS) on security management systems, best practice for implementing supply chain security, requirements for bodies providing audit and certification of supply chain security management systems, and others topics. Applicable ISO/PAS includes ISO/PAS 17712, ISO/FDIS 18185, ISO/IEC 18000, ISO/PAS 28001, and ISO/PAS 28003.[14]

Smart and Secure Trade Lanes (SST): The ultimate goal of SST, based on the Radio Frequency Identification (RFID), is to enhance the visibility of each container shipment, as well as the transparency of those shipments within the overall supply chain; improve the physical security of containers and their contents; and create an audit trail that enables the system to analyze, learn, and adjust to dynamic changes.[15]

3. Maritime Supply Chain Security

Maritime security dates back to early maritime history under the themes of piracy and cargo theft and now includes also stowaways, people and drug trafficking, information security, and, of course, maritime terrorism after the 9/11 events.[16] Nations have a common interest in achieving two complementary objectives: to facilitate the vibrant maritime commerce that underpins economic security, and to protect against ocean-related terrorist, hostile, criminal, and dangerous acts.[17] In the simplest form, international supply chain security requires that

[13] US Government Accountability Office, ***Report to Congressional Requesters: Supply Chain Security-DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports***, 2013, p. 12.
[14] US Department of Homeland Security, ***ibid***, 2007, p. 84.
[15] Thomas A. Cook, ***Managing Global Supply Chains: Compliance, Security, and Dealing with Terrorism***, Auerbach Publications, Boca Raton, FL., 2008, p. 116.
[16] Vinh V., Thai, "Effective Maritime Security: Conceptual Model and Emprical Evidence" ***Maritime Policy and Management***, Vol. 36, No. 2, 2009, 147-163, p. 147.
[17] US Department of Homeland Security, ***The National Strategy for Maritime Security***, 2005b, p. 2.

the cargo is secure from the point of origin, and that it remains secure during transit until the point of deconsolidation and domestic distribution.[18] Clearly, any measures adopted must cover the whole of the international logistics supply chain and not just the shipping component of such distribution channels.[19]

Threats to maritime security are labeled variously by different resources. Hansen proposes the "Four Circles Model" which maritime security threats are labeled as "piracy", "terrorism", "insurgency", and "organized crime".[20] On the other hand, Department of Homeland Security (DHS) groups the maritime security threats as "nation state threats", "terrorist threats", "transnational criminal and piracy threats", "environmental destruction", and "illegal seaborne immigration".[21]

Although the total threat picture in the maritime domain consists of a number of levels of threats that are distinctive and that represent different types of criminal activities directed toward the maritime sector, terrorism has been the most widely discussed maritime security threat in international media as well as in expert studies by academics, think tanks, and analytical institutes since 2000.[22]

4. Maritime Supply Chain Security Measures

The hijacking of the Italian cruise ship "Achille Lauro" and the killing of a disabled American tourist in October 1985 marked one of the first terrorist acts in maritime history.[23] As a result, IMO developed "The Convention for the Suppression of Unlawful Acts against the

[18] US Department of Homeland Security, ***ibid*** , 2007, p. 27.
[19] Peter B. Marlow, "Maritime Security: An Update of Key Issues", ***Maritime Policy and Management***, 2010, Vol. 37, No. 7, 667-676, p. 675.
[20] Hans T. Hansen, "Distinction in the Finer Shades of Gray: The 'Four Circles Model' for Maritime Security Threat Assessment", Rupert Herbert-Burns, et. al., (ed.), ***Lloyd's MIU Handbook of Maritime Security***, CRC Press, London, 2008, 73-83, p. 75.
[21] US Department of Homeland Security, ***The National Strategy for Maritime Security***, 2005c, pp. 3-6.
[22] Hans T. Hansen, ***ibid,*** p. 74.
[23] Peter B. Marlow, ***ibid***, p. 670.

Safety of Maritime Navigation (SUA)" to ensure that appropriate action is taken against persons committing unlawful acts against ships.[24] Nevertheless, most of the security measures currently enforced in the maritime domain are the results of heightened security threat perceptions after September 2001.[25] After 9/11 attacks, United States-led national security initiatives were followed by United Nation-led multilaterally security initiatives and industry-led security initiatives.

5. Two Axes Multi-Sector (TAMS) Model Approach to the Maritime Supply Chain Security

Supply chain links many companies together, starting with the unprocessed raw materials and ending with the final customer using the finished goods. Attempts to overcome the independent efforts of the firms at optimizing their logistical systems have resulted in the creation of Maritime Supply Chain Management (MSCM).[26] Security in a supply chain is an important Supply Chain Management (SCM) issue and it should be achieved with a holistic approach. This approach includes the security quality in all processes of SCM and prevention from source rather than the final inspection.

Different perspectives have been put forward to achieve the international supply chain security. The Organization for Economic Cooperation and Development (OECD) has broken down the complex web of supply chain into three principal flows.[27] Willis and Ortiz have asserted three perspectives on the supply chain.[28] Department of Homeland Security (DHS) has described a framework in terms of four

[24] Devinder Grewal, "International Ship Safety Regulations", Wayne K. Talley, (ed.), ***Maritime Safety, Security and Piracy***, Informa, London, 2008, 11-30, p. 13
[25] Prakash Metaparti, ***ibid***, p. 723.
[26] Ruth Banomyong, "The Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management" ***Maritime Policy and Management***, 2005, Vol. 32, No. 1, 3-13, p. 4.
[27] OECD, ***Security in Maritime Transport: Risk Factors and Economic Impact***, OECD, Paris, 2003, p. 24.
[28] Henry H. Willis and David S. Ortiz, ***Evaluating The Security Of The Global Containerized Supply Chain***, RAND Corporation, Santa Monica, CA., 2004, p. 14.

parts to achieve the international supply chain security.[29] Finally, Bichou, and Bichou and Evans have used the multi-channel layered approach.[30]

Various movements throughout the supply chain in the four different points of view are shown in Table 1.

In addition to these approaches to the supply chain security in a horizontal manner, "The National Strategy for Maritime Security of DHS" and "its plans" introduce a "Multi-Layered Risk Based Management" approach to the supply chain security in a vertical manner.[31] These layered measures seek to protect the three phases of the maritime commerce chain –"overseas", "in-transit", and "on the US shores"- each of which has different jurisdiction zones and rules.

[29] US Department of Homeland Security, ***ibid*** , 2007, p. 27.

[30] See Khalid Bichou, "Review of Port Performance Approaches and a Supply Chain Framework to Port Performance Benchmarking", Mary R. Brooks and Kevin Cullinane, (ed.), ***Devolution, Port Governance and Port Performance, Research in Transportation Economics***, Volume 17, JAI Press, The Netherlands, 2007, 567-598, p. 586; Khalid Bichou, "Security and Risk-Based Models in Shipping and Ports: Review and Critical Analysis" discussion paper no. 2008-20, ***the OECD/ITF Round Table of 11-12 December 2008 on Security, Risk Perception and Cost-Benefit Analysis***, 2008, p. 19; Khalid Bichou and Andrew Evans, "Maritime Security and Regulatory Risk-Based Models: Review and Critical Analysis", Khalid Bichou, et. al., (ed.), ***Risk Management in Port Operations, Logistics and Supply Chain Security,*** Informa Law, New York, NY, 2007, 265-281, p. 271.

[31] See US Department of Homeland Security, 2005b, ***ibid,*** p. 13, 20; US Department of Homeland Security, ***ibid***, 2005c, p. B-1; US Department of Homeland Security, 2007, ***ibid***, p. 10.

Table 1: Multi-Channel Approaches to the Maritime Supply Chain Security

OECD	Willis and Ortiz	DHS	Bichou; Bichou and Evans
Movement of goods	Logistics network	Secure cargo	Logistics channel (vessels) Trade Channel (cargo)
Movement of custody	Transition network	Secure transit	Supply channel
Movement of information	-	Accurate data and information sharing	*Note 1
-	Oversight system	Standards and regulations	Trade Channel

*Note 1: Information flows occur between all three channels.
Physical and payment flows only occur between logistics and supply channel.

In this study, Two Axes Multi-Sector (TAMS) approach is introduced to achieve the international supply chain security in horizontal and vertical manners simultaneously. TAMS model composes a number of sectors on the x-y plane.

Two different horizontal (throughout the x-axis) flows of security are introduced in the TAMS model against the y-axis, as 'cargo flow security' and 'transit flow security'. These two flows run in the logistics channel throughout the supply chain (Figure 1).

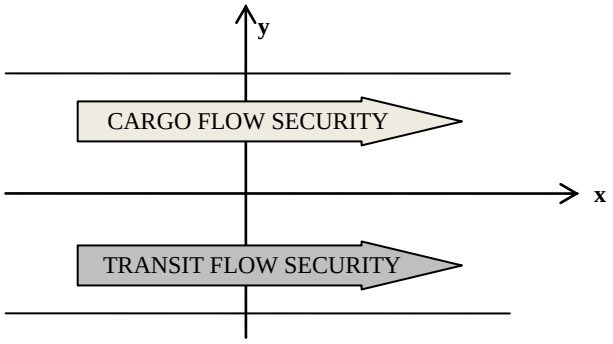


Figure 1: Horizontal Flows in TAMS Model

"Cargo flow security" includes the security of container, break bulk, or bulk cargo, and also, information about the cargo flowing before, after or at the same time with the cargo electronically or by hand (e.g., bill of lading, delivery order, warehouse receipt, customs documents, cargo manifest, etc).

"Transit flow security" includes the security of the dynamic assets (vessels), stationary assets, which host the vessels and cargo awhile (e.g., ports, warehouses, logistics centers, container freight stations, etc.), and the information flowing regarding these assets (e.g., Notice of Readiness (NOR), statement of facts and time sheet, warehouse management system data, etc). Custody is altered number of times along the flow and there are a lot of people contact with the dynamic and stationary assets and cargo in the flow.

TAMS model has a number of vertically separated layered parts (throughout the y-axis) against the x-axis, which are the mixture of physical and legal zones of jurisdiction, for enhancing the security (Figure 2).

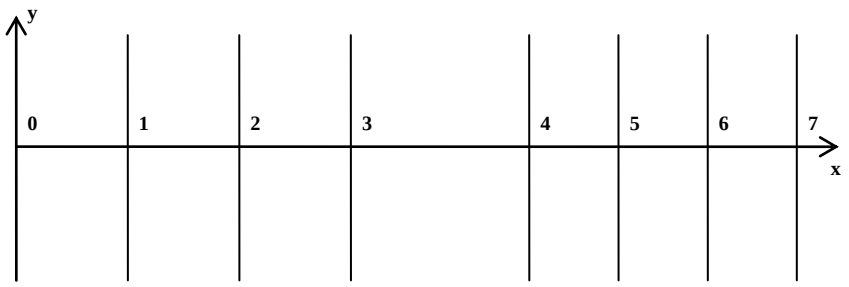


Figure 2: Vertical Layers of TAMS Model

As a result, TAMS model composes seven different sectors, each of which has two sub-sectors, on the x-y axes (Figure 3). Each sector has different jurisdiction and regulation on its own flow.

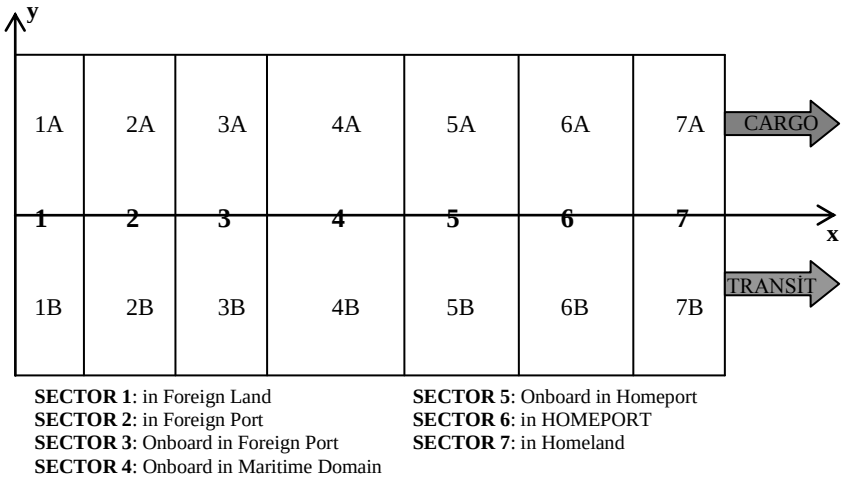


Figure 3: TAMS Model

Sector 1 and Sector 7 are subject to the sovereignty of the states. States have national jurisdiction to make security regulations related to the cargo, vessels, facilities, and information in these sectors.

States have the sovereignty in Sector 2 and Sector 6 that are the port zones. Cargo waits to be loaded to the ship in Sector 2, and waits for exiting from the port in Sector 6. Cargo security is provided by the regulations in the port. Port security is subject to the national regulations and the International Ship and Port Facility Security (ISPS) Code if the state is a participant of this Code.

Cargo is onboard in Sector 3 and Sector 5. Cargo security is provided by the vessel crew in accordance with the flag state and ISPS Code regulations. Vessel security is subject to the flag state's sovereignty and depends on its national laws and the ISPS Code if the

flag state is a participant of the ISPS Code. Port states may contribute the security of vessel by taking additional measures inside the port. Port states also have the Port State Control (PSC) authority to control the vessel security in accordance with the ISPS Code.

In the port zone, the coastal state can inspect a foreign ship as a PSC authority and it can prevent her from exiting its port in a non-seaworthiness condition.

Sector 4 is the maritime domain that consists of the different sea zones. These zones are determined by the international law of the sea which assigns different national or international jurisdiction to them. United Nations Convention on the Law of the Sea of 1982 (UNCLOS) is the current agreement which codified the law of the sea in the world. Most of the rules of this agreement have also become a generally accepted rules and standards for the states other than contracting countries. Understanding the rights and jurisdiction in these zones is important for supply chain security, because the terrorists can benefit from the freedom of navigation in the maritime domain.

According to the 1982 UNCLOS, the sea zones related to the maritime transportation in a logistics channel are "internal waters", "territorial sea", "contiguous zone", "Exclusive Economic Zone (EEZ)" and "high seas". A country has sovereignty on its "internal waters" and "territorial sea" but its jurisdiction is restricted in such conditions like the innocent passage.[32] A foreign ship has a freedom of navigation if compatible with the innocent passage regulations when she sails through the territorial sea and the internal waters of a coastal state for a port call. But a coastal state may exercise the control necessary related to its custom, fiscal, immigration, or sanitary laws and regulations within its contiguous zone. This zone may extend beyond 24 nautical miles from the baselines,[33] which means it also includes the territorial sea.

---

[32] United Nations (UN), ***UN Convention on the Law of the Sea of 1982 (UNCLOS),*** 1982, article 21.2.
[33] United Nations, ***ibid***, article 33.

The EEZ is an area beyond and adjacent to the territorial sea, subject to both the rights and jurisdiction of coastal state and the rights and freedoms of other states.[34] As related to maritime transportation, all states enjoy the freedom of navigation in the EEZ of a coastal state.[35] But the coastal state has the right to inspect and detent a ship in accordance with its law in case of a maritime pollution from the vessel.[36] The high seas, as another zone, are open to all states and they enjoy the freedom of navigation.[37]

6. The US Maritime Supply Chain Security

6.1. The Cornerstones of the US Legal Structure

Homeland Security Presidential Directive (HSPD)-3: Homeland Security Advisory System (HSAS) (replaced by the National Terrorism Advisory System (NTAS) in 2011).

HSPD-5: Management of Domestic Incidents, National Incident Management System (NIMS).

HSPD-7: National Infrastructure Protection Plan (NIPP), Transportation Systems Sector Specific Plan (TS SSP) (which is one of the Critical Infrastructure and Key Resources (CIKR) of the NIPP) and its Maritime Mode Annex.

HSPD-8: National Preparedness Goal.

National Security Presidential Directive (NSPD)-41/HSPD-13: National Strategy for Maritime Security (NSMS) and its eight plans.

Intelligence Reform and Terrorism Prevention Act of 2004 (amends the US code of Title 49): National Strategy for Transportation Security and transportation modal security plans.

Maritime Transportation Security Act (MTSA) of 2002: National Maritime Transportation Security Plan (NMTSP) (superseded due to

[34] United Nations, ***ibid***, article 55.
[35] United Nations, ***ibid***, article 58.
[36] United Nations, ***ibid,*** article 220.5.6.
[37] United Nations, ***ibid***, article 87.

the maritime mode annex of TS SSP which serves concurrently as the NMTSP[38]), Area Maritime Transportation Security Plans, Vessel and Facility Security Plans, and Automatic Identification System (AIS) requirements for vessels which are excluded by the "Regulation 3-Exceptions" of the "International Convention for the Safety of Life at Sea (SOLAS)".

Security and Accountability for Every (SAFE) Port Act of 2006: Strategic Plan to Enhance International Supply Chain Security.

6.2. Main Elements of the US Organizational Structure

Organizational structure of the US maritime supply chain security was reconstituted after 9/11. Department of Homeland Security (DHS) was established to prevent terrorism and enhance security, manage the US borders, administer immigration laws, secure cyberspace, and ensure disaster resilience in March 2003. The US Customs Service, formerly under the direction of Department of the Treasury since its creation in 1789, was transferred to the DHS in March 2003 and renamed as the Bureau of Customs and Border Protection (CBP).[39] Transportation Security Administration (TSA) was established by the Aviation and Transportation Security Act of 2001, and the US Coast Guard (USCG) under the Department of Transportation (DOT) was moved under the DHS. Maritime Administration (MARAD) of DOT was responsible together with the DHS as the MTSA of 2002 was adopted. Also, Department of Energy (DOE) and National Nuclear Security Administration (NNSA) serve the supply chain security in accordance with the illicit traffic of nuclear and other radioactive materials.

6.3. Findings from the TAMS Model

The means regarding the US maritime supply chain security are presented in the Figure 4 by using the TAMS model.

---

[38] US Department of Homeland Security (DHS), ***Transportation Systems Sector Specific Plan: An Annex to the National Infrastructure Protection Plan***, 2010, p. 169.
[39] Thomas A. Cook, ***ibid***, p. 19.

6.3.1. Findings in the Overseas Side of the Maritime Supply Chain

Automated Targeting System (ATS) is used for screening the containers. It uses "manifest and entry declaration data" from Automated Commercial System and "enforcement data" from Treasury Enforcement Communications System to provide targeting functionality for cargo.[40]

6.3.2. Findings in the Maritime Domain of the Maritime Supply Chain

The most important means for the maritime security are Long-Range Identification and Tracking (LRIT) and Automatic Identification System (AIS). These systems provide advanced Maritime Domain Awareness (MDA). As it was adopted by International Maritime Organization (IMO) in 2001, AIS was initially and specifically designed as an aid to safe navigation and collision avoidance. Then security quickly became its main role.[41] So, AIS has some security gaps due to open broadcast, restricted range, and altering the settings or input information. To fill in the huge gap between areas of AIS coverage, LRIT regulation (proposed by the US in 2002 and adopted by IMO in 2006) came into force. LRIT is a satellite-based closed system designed solely for security, and ships' crew cannot alter settings or input information.[42] Only flag states, port states, and coastal states (within 1000 nautical miles of their coastlines) can receive LRIT information. The USCG also initiated the Nationwide AIS (NAIS) project in response to the "Maritime Transportation Security Act of 2002". The system combines AIS data -such as vessel location, source, and speed- with other government information and sensor data to form a holistic view of maritime vessel traffic near the continental US and its territorial sea.

The United States Coast Guard (USCG) also published a proposed rule with "73 FR 78295" that would expand the applicability

[40] US Department of Homeland Security, ***ibid***, 2007, p. 70.
[41] Martin N. Murphy, "Lifeline or Pipedream? Origins, Purposes, and Benefits of Automatic Identification System, Long-Range Identification and Tracking, and Maritime Domain Awareness", Rupert Herbert-Burns, et. al., (ed.), ***Lloyd's MIU Handbook of Maritime Security***, CRC Press, London, 2008, 13-28, pp.1 4-24.
[42] Martin N. Murphy, ***ibid***, pp. 17-18.

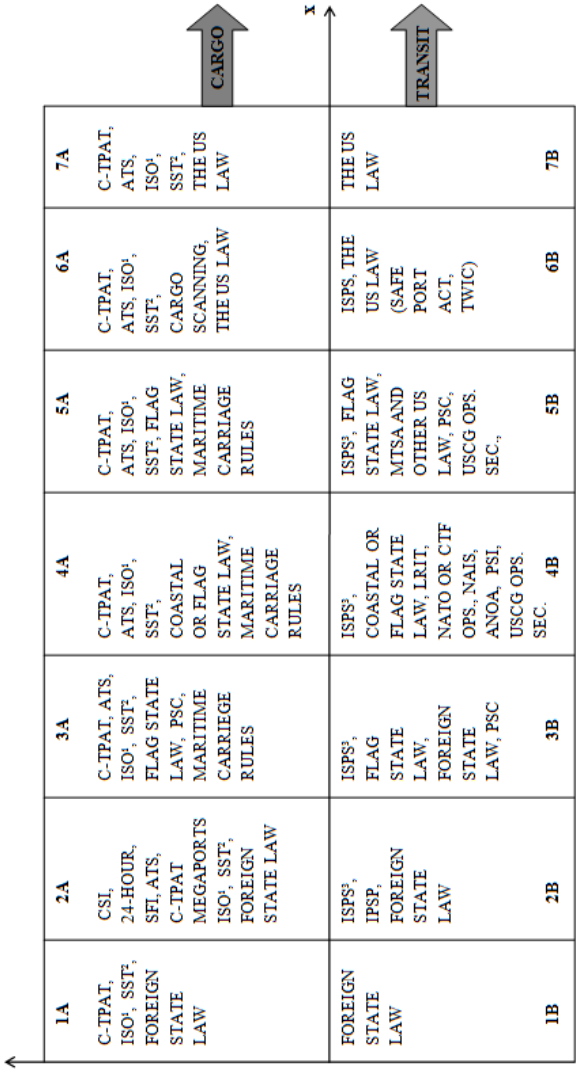
of AIS requirements beyond the USCG Vessel Traffic Service (VTS) areas to all US navigable waters in 2008 and require it for some of vessels which are excluded by the "Regulation 3-Exceptions" of the "International Convention for the Safety of Life at Sea (SOLAS)". Department of Homeland Security (DHS) also deploys the 'Small Vessel Security Strategy (SVSS)' in order to enhance Maritime Domain Awareness (MDA) by leveraging a strong partnership with the small vessel community and public and private sectors.[43]

The other means of maritime security in the maritime domain are the USCG operational security using the Maritime Security Risk Analysis Model (MSRAM) and Advanced Notice of Arrival (ANOA). According to the US code of "Title 33-Navigation and Navigable Water", each ship whose voyage time is 96 hours or more submits an ANOA at least 96 hours before entering the port or place of destination. Also North Atlantic Treaty Organization (NATO), regional or other allied maritime security operations task forces contribute the MDA.[44]

6.3.3. Findings in the Homeland Side of the Maritime Supply Chain

The Bureau of Customs and Border Protection (CBP) uses Non-Intrusive Inspection (NII) technology- that includes large-scale X-ray and Gamma-ray imaging systems, as well as a variety of portable and handheld technologies- and radiation scanning technology in the US ports. Also, "MTSA of 2002" is applied to all ships in the ports of the US. Another instrument for port security, in response of "Security and Accountability for Every (SAFE) Port Act of 2006", is the "Transportation Worker Identification Credential (TWIC)" program. TWIC requires background security checks and biometric-based credentials for all those working in or around US ports and ensures that

[43] US Department of Homeland Security, ***Small Vessel Security Strategy***, 2008, p. iv.
[44] Russell Pegg, "Maritime Forces and Security of Merchant Shipping in the Mediterranean Sea and Northern Indian Ocean", Rupert Herbert-Burns, et. al., (ed.), ***Lloyd's MIU Handbook of Maritime Security***, CRC Press, London, 2008, 29-37, p. 29.



SECTOR 1: in Foreign Land **SECTOR 4**: Onboard in Maritime Domain **SECTOR 6**: in HOMEPORT
SECTOR 2: in Foreign Port **SECTOR 5**: Onboard in Homeport **SECTOR 7**: in Homeland
SECTOR 3: Onboard in Foreign Port

Note 1: If the trade partner applies the ISO standards concerned with supply chain security.
Note 2: If the trade partner is a Smart and Secure Trade Lanes (SST) participant. Also, C-TPAT requires the Tier 3 participants to utilize the container security devices (CDS).
Note 3: If the foreign country and/or the country of vessel is a participant of ISPS Code.

Figure 4: The US Maritime Supply Chain Security Means in the TAMS Model

only authorized persons have access to the US ports.[45] Also, from port of entry to the destination point, the USCG requires that vessels carrying certain dangerous cargo report their movements on the inland rivers,[46] and Transportation Security Administration (TSA) provides the highway, rail, and air cargo security with various security initiatives.

7. Maritime Supply Chain Security of Turkey

7.1. The Cornerstones of Turkey's Related Legal Structure

Organization and Duties of Disaster and Emergency Management Presidency Act of 2009 - No: 5902 (Revised in 2014) (5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun): This Act establishes the Disaster and Emergency Management Presidency under the Prime Ministry to manage the duties regarding disasters, emergency, and civil defense.

Regulations on Disaster and Emergency Response Duties (2013) (Afet ve Acil Durum Müdahale Hizmetleri Yönetmeliği): The Regulations rules the state and local (province) Disaster Response Plan to be formed and also rules the establishment of state and local Disaster and Emergency Management Centers.

Regulations on Duties regarding Chemical, Biological, Radiological, and Nuclear (CBRN) Hazards (2012) (Kimyasal, Biyolojik, Radyolojik ve Nükleer Tehlikelere Dair Görev Yönetmeliği): The Regulations rules the prevention, preparedness, response, and recovery of CBRN hazards.

Customs Act of 1999 - No: 4458 (revised in 2014) (4458 sayılı Gümrük Kanunu): This law introduces the basic rules about Authorized Economic Operator (AEO), customs risk analysis, and summary declaration (24-hours rule).

Customs Regulations of 2009 (revised in 2015) (Gümrük

---

[45] C. Ariel Pinto, et. al., "US Port Security", Wayne K. Talley, (ed.), ***Maritime Safety, Security and Piracy***, Informa, London, 2008, 217-233, p. 220.
[46] US Department of Homeland Security, 2007, ***ibid***, p. 77.

Yönetmeliği): The Regulations introduces the detailed rules about risk analysis, summary declaration (24-hours rule), and radiation controls.

Regulations on Facilitation of Customs Procedures of 2014 (Gümrük İşlemlerinin Kolaylaştırılması Yönetmeliği): AEO procedures for exporters were formed by the Regulations.

Ports Act of 1923 - No: 618 (revised in 2008) and its Ports Regulations of 2012 (revised in 2015) (618 sayılı Limanlar Kanunu ve Limanlar Yönetmeliği): This Act and Regulations require the ships to submit an Advance Notice of Arrival (ANOA) at least 24 hours before entering the Turkish ports.

Guidelines on Maritime Traffic Regulations for the Turkish Straits (1998) (Türk Boğazları Deniz Trafik Düzeni Tüzüğü): This Guidelines requires owners, masters, or agents of the vessels with dangerous cargo or the vessels of 500 GRT (gross register tonnage) and upwards to submit "Sailing Plan 1" in writing to the nearest Traffic Control Center in IMO standard format as defined by the Administration at least 24 hours before the vessel's arrival at İstanbul or Çanakkale Straits.

Regulations on Application of the International Ship and Port Facility Security (ISPS) Code (2007) (Uluslararası Gemi ve Liman Tesisi Güvenlik Kodu Uygulama Yönetmeliği): The Regulations translates the international security requirements arising from the ISPS code into the national legislation.

Regulations on the Declarations Arising from the Safety of Life at Sea (SOLAS) and the Prevention of Pollution from Ships (MARPOL) Agreements (2006) (SOLAS ve MARPOL Sözleşmelerine Göre Bildirimlere İlişkin Yönetmelik): The Regulations requires the stakeholders to submit the declarations arising from the ISPS Code (Chapter XI-2 of SOLAS), as well as the MARPOL 73/78 and the other chapters of SOLAS 74.

Communiqué on Installation and Specification of Automatic Identification System (AIS) Class-B CS (2007) (revised in 2009) (Otomatik Tanımlama Sistemi (AIS) Klas B CS Cihazının Gemilere Donatılmasına ve Özelliklerine Dair Tebliğ): AIS Class-B CS is mandated for some

vessels which are excluded by the "Regulation 3-Exceptions" of the "International Convention for the Safety of Life at Sea (SOLAS)".

7.2. Main Elements of Turkey's Organizational Structure

Various ministries have the operational authority to provide the security of maritime supply chains in Turkey. Undersecretariat of Public Order and Security under Prime Ministry produces policies and strategies and facilities coordination between relevant institutions in the field of counterterrorism. It has no operational duties.

Directorate General of Customs and Directorate General of Customs Enforcement serve under the Customs and Trade Ministry. Another ministry responsible for maritime supply chain security is the Ministry of Transport, Maritime Affairs and Communications (MTMAC). Directorate General of Maritime and Inland Waters Regulation (DGMIWR) under this Ministry has a wide range of responsibility including authorizing and controlling the maritime partners, such as ports, port facilities, shipping agencies, freight forwarders etc., identifying the seafarers' and marine workers' vocational qualification and examining, identifying minimum safety, security, and environmental standards for vessels, and certifying and surveying, giving PSC and Flag State Control services, and registering ships. Second institution under the same Ministry is the Directorate General of Coastal Safety, which is responsible for operating the Vessels Traffic System (VTS), LRIT, and AIS.

Another agency is the Turkish Coast Guard Command (TCG), which is a naval force under the Ministry of Interior. TCG is to protect the Turkish coastal water and maritime domain by its law enforcement authority. TCG controls the vessels' compliance with the ISPS Code and the other maritime security requirements outside the Port Administrative Border (PAB). Inside the PAB, DGMIWR under the MTMAC has this authority. The most important handicap for Turkey's maritime security is that TCG is not authorized to collect intelligence, although it has the responsibility of sea area of 377.714 square kilometers.

Turkish National Police (TNP) under the Ministry of Interior is responsible for preventing the terrorist acts and performing the passport

control in the port zone. Also, Turkish Atomic Energy Authority under the Prime Ministry contributes the other authorities in case of a Chemical, Biological, Radiological and Nuclear (CBRN) threat.

7.3. Findings from the TAMS Model

The means regarding the maritime supply chain security of Turkey are presented in Figure 5 by using the TAMS model.

7.3.1. Findings in the Overseas Side of the Maritime Supply Chain

Turkey has not had an Authorized Economic Operator (AEO) regulation for the importers yet. AEO was only regulated for the exporters. On the other hand, cargo is screened via the BILGE (Bilgisayarlı Gümrük Etkinlikleri - Computerized Customs Activities) system and risk assessment is performed by the Customs. A 'do not load' message will be issued to the port of origin, if required.

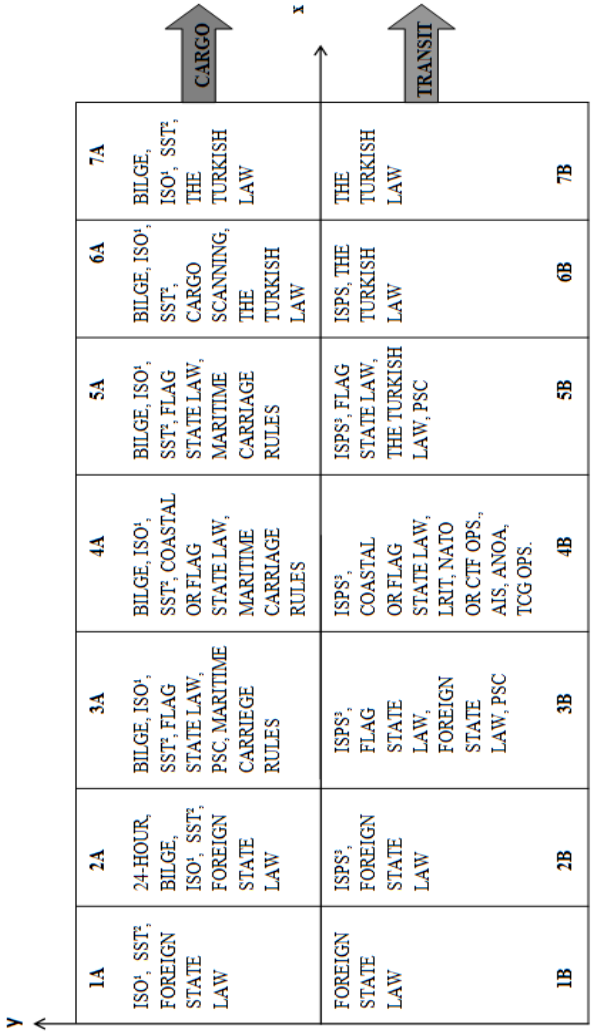
7.3.2. Findings in the Maritime Domain of the Maritime Supply Chain

Turkey established the AIS in 2007 and LRIT in 2009 (tested by IMO in 2010). Turkey also requires some of the vessels, which are excluded by the "Regulation 3-Exceptions" of the "International Convention for the Safety of Life at Sea (SOLAS)" to install the AIS Class B-CS equipment with a Communiqué in 2007.

Also, Turkish Navy is the participant of NATO Operation Active Endeavour which aims to deter and disrupt terrorist activity in the Mediterranean Sea and the participant of Combined Task Force 150 (CTF-150) which is a purely voluntary multinational task force and which aims to promote maritime security in order to counter terrorist acts and related illegal activities, and also the participant of Combined Task Force 151 (CTF-151) which is a multinational force under the authority of United Nations Security Council Resolutions and which aims to disrupt piracy and armed robbery at sea.

7.3.3. Findings in the Homeland Side of the Maritime Supply Chain

Turkish Customs scans the cargo by using container scanning devices. The security of the maritime supply chain from the port to the destination point is provided by Turkish National Police (TNP) or the Turkish Gendarmerie in accordance with their area of responsibility.



SECTOR 1: in Foreign Land
SECTOR 2: in Foreign Port
SECTOR 3: Onboard in Foreign Port
SECTOR 4: Onboard in Maritime Domain
SECTOR 5: Onboard in Homeport
SECTOR 6: in HOMEPORT
SECTOR 7: in Homeland

Note 1: If the trade partner applies the ISO standards concerned with supply chain security.
Note 2: If the trade partner is a Smart and Secure Trade Lanes (SST) participant.
Note 3: If the foreign country and/or the country of vessel is a participant of ISPS Code.

Figure 5: Maritime Supply Chain Security Means of Turkey in the TAMS Model

8. Comparison of the Maritime Supply Chain Security of the US and Turkey by Using the TAMS Model

Sector 1: In Sector 1A, the US uses the Customs-Trade Partnership against Terrorism (C-TPAT) initiative to provide the security of cargo flow. Also, Tier 3 participants of C-TPAT are required to use the container security devices. This requirement will also be able to stimulate the Tier 3 participants to attend the Smart and Secure Trade Lanes (SST) initiative. Turkey does not have an Authorized Economic Operator (AEO) regulation for its importers. Therefore, a supply chain security gap occurs in just the beginning of its supply chain.

In Sector 1B, the US requires the C-TPAT participants to perform risk analysis by using appropriate systems or consulting firms in their supply chains. Although the foreign state has jurisdiction in the transit flow, risk analysis requirement makes the transit flow secure since the security of facilities, warehousing, transportation, etc. is analyzed by the participants. The transit flow security of Turkey depends on the foreign state security precision due to the lack of AEO regulation for its importers.

Sector 2: Ultimate aim of all maritime security strategies of the US is to push the border outward by preventing the threats at overseas. So, in Sector 2A, the US screens and scans the cargo in the foreign port via various means such as Container Security Initiative (CSI), Megaports, Secure Freight Initiative (SFI), 24-hour rule, and Automated Targeting System (ATS). On the other hand, Turkey has imposed the 24-hour rule and established the BILGE system to screen the cargo overseas, but it still scans the cargo after the cargo enters its homeland. Therefore, it has a greater risk of a terrorist attack in homeland or smuggling providing fund for terrorist.

In Sector 2B, the US officials visit the foreign ports via the International Port Security Program (IPSP) and control the compliance with the ISPS Code to provide the transit flow security. Unless the port complies with the ISPS Code, vessels departing from that port are not allowed to enter the US port, or they are required strict security

measures. Turkey does not have a foreign port visit policy, so a maritime security gap is arisen.

Sector 3: In Sector 3A, cargo flow security level of both the US and Turkey is protected like their security level provided in Sector 1A and 2A, but, of course, dependable seafarers are essential for this protection. If the flag state of vessel is a participant of International Labor Organization (ILO) Seafarers' Identity Document Convention, it will be helpful for the security. In Sector 3B, the maritime security of both countries depends on the precision of the port state and flag state of vessel on the maritime security.

Sector 4: In Sector 4A, the security level of cargo flow for both the US and Turkey is conserved like the security level in the previous Sectors. In Sector 4B, The US signed bilateral ship boarding agreements with more than a hundred countries via the Proliferation Security Initiative (PSI). The US also establishes the Long-Range Identification and Tracking (LRIT) and Nationwide Automated Identification System (NAIS). NAIS provide a Common Operational Picture (COP). The 96-hours Advance Notice of Arrival (ANOA) rule was imposed to improve the operational security. The United States Coast Guard (USCG) uses the Maritime Security Risk Analysis Model (MSRAM) to identify the High Interest Vessels (HIVs) and suspected vessels. Deployable Operations Group (DOG) was established by the USCG to improve the operational security and the USCG deploys the Maritime Safety and Security Team (MSST) under the DOG as required.

On the other hand, Turkey integrates its LRIT, Vessel Traffic Service (VTS) and AIS, but this integration does not include the required maritime security intelligence from the other related governmental institutions. This is a handicap to be obtained an effective COP on behalf of the maritime security. The 24-hours ANOA is perceived only as a maritime safety issue and declared to the Directorate General of Maritime and Inland Waters Regulation (DGMIWR). Turkish Coast Guard (TCG) know very little about the security level of the arriving vessels due to the lack of an effective nationwide COP**.** Probably, due to the inefficient COP and lack of intelligence, TCG has not needed to establish a maritime security risk

analysis model for vessels in the maritime domain. Also, the Operation Security Units (DAGOT) of the TCG does not have enough personnel proficiency and equipment technology compared with those of US. Nonintegrated information and intelligence, grey areas of responsibility between the agencies, and inefficient organization structure cause a very important security gap in Sector 4B for Turkey.

Both the US and Turkey require some of the vessels which are excluded by the "Regulation 3-Exceptions" of the "International Convention for the Safety of Life at Sea (SOLAS)", especially engaged in commercial service, to install AIS Class B. But measures are still needed to be taken for non-commercial vessels. The US deployed the Small Vessel Security Strategy (SVSS) for small vessels as a measure, but Turkey does not have this kind of strategy and still has a security gap against a terrorist attack using a recreational boat.

Both countries declare dangerous zones and restricted areas for their gas terminals, and require waterborne escorts to the vessels carrying certain dangerous bulk cargo in their waterways to prevent a ramming attack using a Waterborne Improvised Explosive Device (WBIED).

Sector 5: In Sector 5A, the security level of cargo flow for both the US and Turkey is conserved like the security level in the previous Sectors. In sector 5B, the USCG controls the vessel for the ISPS Code compliance by its Port State Control (PSC) authority. Also, it has the authority to conduct boarding the vessel in case of a terrorist threat. In Turkey, DGMIWR has the PSC authority and Turkish National Police (TNP) is responsible for a terrorist threat arising from the vessel in Sector 5B.

***Sector 6*:** According to the Department of Homeland Security (DHS), the measure of effectiveness for the Radiation Portal Monitors (RPM) and Non-Intrusive Inspection (NII) program is 'to deploy RPM and NII devices to scan at least 98% of containers entering the US by sea'.[47] On the other hand, Turkey continues to obtain NII and RPM

[47] US Department of Homeland Security, 2007, ***ibid***, p. 82.

devices, but it has a disadvantage due to its limited budget and inefficient technological capacity at producing this kind of devices. This issue causes a maritime security gap for Turkey in Sector 6A. In Sector 6B, both Turkey and the US comply with the ISPS Code for their ports. Moreover, the US requires background check and biometric based credential for transportation or port workers via Transportation Worker Identification Credential (TWIC) program. Turkey does not have a similar measure, and this is another security gap for Turkey.

***Sector 7*:** In Sector 7A, high risk due to lack of AEO regulation and inefficient scanning performance causes a very important supply chain security gap for Turkey. In Sector 7B, the US integrates the security of highway, railway, and airway under TSA. C-TPAT also increases the transit flow security in homeland. For Turkey, TNP or the Turkish Gendarmerie is responsible for the railway and highway security. Lack of AEO program for importers also may cause a security gap in Sector 7B.

9. Conclusion

In this study, the maritime supply chain security gaps that Turkey, which is a middle power, encounters are examined by comparing with the maritime supply chain security of the US, which is the dominant power. The maritime supply chain security gaps of Turkey revealed by benchmarking in the TAMS model are as follows:

- Not to be able to scan cargo in overseas,
- Not to be able to visit foreign ports for controlling the ISPS Code compliance,
- Inefficient number of cargo scanning devices,
- Lack of AEO regulations for its importers,
- Non-integrated maritime security intelligence,
- Inefficient legal and organizational structure, gray areas of responsibility between the institutions, and therefore inter-institution power struggle,
- Lack of intelligence authority of the TCG, although it has the sea area of responsibility of 377.714 square kilometers, and therefore

the lack of sufficient Maritime Domain Awareness (MDA),

- Lack of non-commercial small vessels awareness in the maritime domain, and
- Lack of port and transportation workers identification system.

To overcome the first two gaps, an international effort is needed, because middle powers are usually developing countries and they have limited productivity and political capacity to influence the behavior of other nations. Unfortunately, the dominant power, the US, and international organizations have not sufficiently contributed to the maritime supply chain security of middle and small powers, although shutdown of the MTS of these nations affects the world trade entirely (e.g., Turkish Straits or Suez Canal). Therefore, Container Security Initiative (CSI) and International Port Security Program (IPSP) should be converted to the international level for the important world trade ports and an international institution should be established to operate and fund to the system.

The third security gap is related to the budget of a middle power. Middle powers have limited budget and they cannot allocate sufficient budget for maritime supply chain security needs. Therefore, the UN organizations or the dominant power and great powers should grant or fund the middle and small powers for their maritime supply chain security needs, especially expensive ones, such as NII and radiation scan devices by globally concerning with the maritime supply chain security.

The forth security gap is resulted from the preference of trade facilitation rather than security, because middle powers are developing countries, and they need income to continue their development. As seen in Turkey's example; AEO program -which was originally developed for supply chain security in the world- was regulated for exporters only, whereas supply chain, trade of importers, security is mainly important for a country's security. AEO is a win-win program, in which the state improves its homeland security and in return importers facilitate their trade. In other words, Customs outsource certain security functions to its trusted industry partners. Unless AEO program regulations include the requirements regarding the self risk

assessment system on the supply chains of importers, it cannot be obtained anything in behalf of public from AEO program.

The other five security gaps are arisen from the inefficient political capacity of the middle powers. Middle powers usually cannot constitute its legal and organizational structure in accordance with its maritime supply chain security needs. This issue results in emergence of many institutions related to the maritime supply chain security with different vision, gray areas of responsibility, and therefore results in inter-institutional power struggle.

Özet

Günümüzün dominant gücü olan ABD, 11 Eylül sonrası retorik dönem olarak adlandırılan dönemde, gerek uluslararası toplumu uluslararası anlaşmaların ve uygulamaların yapılmasına zorlayarak gerekse kendi ulusal kanunlarını çıkararak deniz ulaştırma sisteminin güvenliği alanında paradigmayı değiştirmiş ve bu suretle güvenlik açıklarını kapatmayı hedeflemiştir. Küresel ticaretin hacim olarak %80'inin ve değer olarak %70'inin deniz yolu ile taşındığı ve limanlarda elleçlendiği göz önüne alındığında, lojistik kanalın temel elemanı olan deniz ulaştırma sisteminin ve güvenliğinin önemi ortaya çıkmaktadır. Oysaki orta güçlerin tek başına gerek ulusal gerekse uluslararası ölçekte deniz tedarik zincirleri için yeterli güvenlik önlemlerini alacak güçleri ve etkileri bulunmamakta; bu da gerek söz konusu ülke için gerekse küresel ticaret için güvenlik açıkları oluşturmaktadır.

Organski ve Kugler tarafından formüle edilen Güç Geçişi Kuramı'na (*Power Transition Theory*) göre, dominant güç, hegemon güç olmayıp üstünlüğü kabul edilen en güçlü uluslararası lider ülkedir. Çoğunlukla dominant ülke "*status quo*"yu oluşturur ve savunur. Orta güçler ise talepleri görmezden gelinemeyecek, fakat küresel hiyerarşiyi etkileme gücü olmayan ülkelerdir.

Bu makalenin amacı, orta güç Türkiye ve dominant güç ABD'nin deniz tedarik zincirlerini karşılaştırmak suretiyle dünyadaki orta güçteki ülkelerin karşılaşabileceği deniz tedarik zinciri güvenlik açıklarını tespit etmektir. Bu karşılaştırma için tedarikçiden son kullanıcıya kadar

olan lojistik kanalda yük akışı ve transit akış olmak üzere iki akış boyunca çok sektörlü güvenlik analizine imkân sağlayan İki Eksenli Çok Sektörlü Model (TAMS) geliştirilmiştir.

TAMS modeli ile yapılan karşılaştırma neticesinde, bir orta güç ülkesi olan Türkiye'nin deniz tedarik zinciri güvenlik açıkları; yükün orijin limanında taranamaması, yabancı limanların ISPS Code uygunluğunun tespiti için ziyaret edilememesi, yük tarama cihaz miktarlarının yetersizliği, ithalatçılar için yetkilendirilmiş yükümlü düzenlemesinin olmayışı, deniz güvenliği için istihbarat yapısının bütünleşik olmayışı, yetersiz yasal ve örgütsel yapı, kurumlar arası yetki karmaşası ve bundan kaynaklı kurumlar arası güç mücadelesi bulunması, 377.714 km²'lik sorumluluk sahasına rağmen Sahil Güvenlik Komutanlığı'nın istihbarat toplama yetkisinin olmayışı ve bu sebeple denizde farkındalığın yetersizliği, ticari olmayan küçük tekneler için deniz güvenliği ile ilgili bir düzenlemenin olmayışı ile liman ve taşımacılık alanında çalışan işçilerle ilgili bir tanımlama sisteminin olmayışı olarak tespit edilmiştir.

Sonuç olarak, orta güçlerin deniz tedarik zinciri güvenlik açıkları üç farklı grup altında toplanabilir. Birinci grup, uluslararası organizasyonların ve dominant gücün öncülüğünde iki taraflı ve çok taraflı güvenlik inisiyatiflerinin küresel olarak tanımlanmasıyla kapatılabilecek güvenlik açıkları; ikinci grup, kapatılması için uluslararası organizasyonların veya dominant gücün maddi yardımının gerektiği güvenlik açıkları; üçüncü grup ise, kapatılması için orta güçlerin deniz tedarik zinciri güvenliği ile ilgili bütünleşik bir vizyona sahip olmasını ve ticareti kolaylaştırma ile güvenlik ihtiyacı arasındaki dengeyi sağlamasını gerektiren güvenlik açıkları şeklindedir.

Bibliography

Books

BICHOU Khalid, "Review of Port Performance Approaches and a Supply Chain Framework to Port Performance Benchmarking", Mary R. Brooks and Kevin Cullinane, (ed.), ***Devolution, Port Governance and Port Performance, Research in Transportation Economics, Volume 17***, JAI Press, the Netherlands, 2007.

BICHOU Khalid and EVANS Andrew, "Maritime Security and Regulatory Risk-Based Models: Review and Critical Analysis", Khalid Bichou, Michael G.H. Bell and Andrew Evans, (ed.), ***Risk Management in Port Operations, Logistics and Supply Chain Security,*** Informa Law, New York, NY, 2007.

COOK Thomas A., ***Managing Global Supply Chains: Compliance, Security, and Dealing with Terrorism***, Auerbach Publications, Boca Raton, FL., 2008.

GREWAL Devinder, "International Ship Safety Regulations", Wayne K. Talley, (ed.), ***Maritime Safety, Security and Piracy***, Informa, London, 2008.

HANSEN Hans T., "Distinction in the Finer Shades of Gray: The 'Four Circles Model' for Maritime Security Threat Assessment", Rupert Herbert-Burns, Sam.

KUGLER Jacek and TAMMEN Ronald L., "Regional Challenge: China's Rise to Power", Jim Rolfe, (ed.), ***The Asia-Pacific: A Region in* Transition**, Asia-Pacific Center for Security Studies, HI, 2004.

LEMKE Douglas and KUGLER Jacek, "The Evolution of the Power Transition Perspective", Jacek Kugler and Douglas Lemke, (ed.), ***Parity and War: Evolutions and Extensions of the War Ledger***, University of Michigan Press, Ann Arbor, MI, 1996.

MURPHY Martin N., "Lifeline or Pipedream? Origins, Purposes, and Benefits of Automatic Identification System, Long-Range Identification and Tracking, and Maritime Domain Awareness", Rupert Herbert-Burns, Sam Bateman, Peter Lehr, (ed.), ***Lloyd's MIU Handbook of Maritime Security***, CRC Press, London, 2008.

ORGANSKI A.F. Kenneth, ***World Politics***, Knopf, New York, NY, 1968.

ORGANSKI A.F. Kenneth and KUGLER Jacek, ***The War Ledger***, University of Chicago Press, Chicago, IL. 1980.
PALLIS Athanasios A. and VAGGELAS George K., "EU Port and Shipping Security", Wayne K. Talley, (ed.), ***Maritime Safety, Security and Piracy***, Informa, London, 2008.
PEGG Russell, "Maritime Forces and Security of Merchant Shipping in the Mediterranean Sea and Northern Indian Ocean", Rupert Herbert-Burns, Sam Bateman, Peter Lehr, (ed.), ***Lloyd's MIU Handbook of Maritime Security***, CRC Press, London, 2008.
PINTO C. Ariel, et. al., "US Port Security", Wayne K. Talley, (ed.), ***Maritime Safety, Security and Piracy***, Informa, London, 2008.
RAHMAN Chris, "Evolving U.S. Framework for Global Maritime Security from 9/11 to the 1000-ship Navy", Rupert Herbert-Burns, Sam Bateman, Peter Lehr, (ed.), ***Lloyd's MIU Handbook of Maritime Security***, CRC Press, London, 2008.
TAMMEN Ronald L., LEMKE Douglas, ALSHARABATI Carole, EFIRD Brian, KUGLER Jacek, STAM III Allan C., ABDOLLAHIAN Mark A. and ORGANSKI, A.F. Kenneth, ***Power Transitions: Strategies for The 21st Century***, Chatham House, New York, NY, 2000.
WILLIS Henry H. and ORTIZ David S., ***Evaluating The Security Of The Global Containerized Supply Chain***, RAND Corporation, Santa Monica, CA., 2004.

Papers

BANOMYONG Ruth, "The Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management" ***Maritime Policy and Management***, 2005, Vol. 32, No. 1.
BICHOU Khalid, "Security and Risk-Based Models in Shipping and Ports: Review and Critical Analysis" discussion paper no. 2008-20, ***the OECD/ITF Round Table of 11-12 December 2008 on Security, Risk Perception and Cost-Benefit Analysis***, 2008.
MARLOW Peter B., "Maritime Security: An Update of Key Issues" ***Maritime Policy and Management***, 2010, Vol. 37, No. 7.
METAPARTI Prakash, "Rhetoric, Rationality and Reality in Post-9/11 Maritime Security", ***Maritime Policy and Management***, 2010, Vol. 37, No. 7.

THAI Vinh V., "Effective Maritime Security: Conceptual Model and Emprical Evidence" ***Maritime Policy and Management***, Vol. 36, No. 2, 2009.

(Semi-)Official Contemporary Documents

OECD, ***Security in Maritime Transport: Risk Factors and Economic Impact***, OECD, Paris, 2003.

UNITED Nations (UN), ***UN Convention on the Law of The Sea of 1982 (UNCLOS),*** 1982.

US Department of Homeland Security, ***International Outreach and Coordination Strategy***, 2005a.

US Department of Homeland Security, ***The National Strategy for Maritime Security***, 2005b.

US Department of Homeland Security, ***International Outreach and Coordination Strategy***, 2005c.

US Department of Homeland Security, ***Strategy to Enhance International Supply Chain Security***, 2007

US Department of Homeland Security, ***Small Vessel Security Strategy***, 2008.

US Department of Homeland Security, ***Transportation Systems Sector Specific Plan: An Annex to the National Infrastructure Protection Plan***, 2010.

US Government Accountability Office, ***Report to Congressional Requesters: Supply Chain Security- DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports***, 2013.