JOURNAL OF MARITIME RESEARCH

Vol XX. No. III (2023) pp 123–132

ISSN: 1697-4840, www.jmr.unican.es

Proposing a Mathematical Dynamic Model to Develop a National Maritime Security Assessment and Build a National Maritime Security Plan

Adriana Ávila-Zúñiga-Nordfjeld[1,*], Marcus Dansarie[2], Hans Liwång[3], Dimitrios Dalaklis[4], Maximo Q. Mejia Jr.[5]

ARTICLE INFO

Article history:
Received 8 Jun 2023;
in revised from 24 Aug 2023;
accepted 03 Sep 2023.

Keywords:
International Ship and Port Facility Security (ISPS) Code, National Maritime Security Plan (NMSP), National Maritime Security Assessment (NMSA), maritime & port security, national security.

ABSTRACT

A proper assessment of maritime security risks at the national level is crucial to a national maritime security plan (NMSP) in order to secure the concerned country's ports, vessels and territorial sea. Thus, the importance of implementing a national maritime security assessment (NMSA) to counter security threats and ensure the continuity of national and international trade. The most important set of international regulations concerning maritime security is the International Ship and Port Facility Security (ISPS) Code, which includes revision, approval and control of compliance of the Port Facility Security Plan (PFSP), which shall be based upon the Port Facility Security Assessment (PFSA). This paper proposes a mathematical dynamic model that calculates in real time the residual risk for the whole country and each of its ports by adapting and expanding the formula and procedures established in the Code, which since it has already been implemented around the world, gives the opportunity to take advantage of this quantitative solution to administrate maritime security risks on a nation-wide basis and create an effective national maritime security plan, which would allow the concerned authorities to improve situational awareness and adapt to security changes through a better planning of human, economic and material resources to deter security threats. The model was tested with the use of five encoded categories as countries, each of them with three ports, which encompassed three port facilities. The results indicate that this methodology is easy to implement and widespread use of that model could strength robustness in national security. .

1. Introduction.

This research effort builds upon a PhD dissertation, which was focused on the subject of "Building a National Maritime Security Policy" (Nordfjeld Avila-Zúñiga, 2018) and a certain number of articles related to this doctoral study strongly associated to maritime and port security.

Despite the increasing number of incidents related to maritime terrorism at sea, piracy and other types of transnational crimes at sea, there is no consensus for a common universal definition of the maritime security concept. Not even the International Maritime Organization (IMO) has provided a clear definition of the term. Some researchers focus on the absence of security threats in the maritime sector, while other authors emphasise the establishment of security measures and the well-functioning of the rule of law to manage risks at sea. Mejia (2007) define maritime security is "the state of being free from

[1]Dr. (Maritime Safety & Security), Associate Senior Lecturer, Swedish Defence University, Department of Systems Science for Defence and Security, Stockholm-Sweden. Adriana.Nordfjeld@fhs.se

[2]PhDc Swedish Defence University, Department of Systems Science for Defence and Security & School of Informatics, University of Skövde, Skövde, Stockholm-Sweden; Marcus.Dansarie@fhs.se.

[3]Dr. Associate Professor, Swedish Defence University, Department of Systems Science for Defence and Security, Stockholm-Sweden, Hans.Liwang@fhs.se.

[4]Dr. (Maritime Safety & Security), Professor, World Maritime University (WMU), Malmö-Sweden, dd@wmu.se.

[5]Dr. Professor, President, World Maritime University (WMU) Malmö-Sweden, op@wmu.se.

[*]Corresponding author: Adriana Ávila-Zúñiga-Nordfjeld. E-mail Address: Adriana.Nordfjeld@fhs.se.

the threat of unlawful acts such as piracy, armed robbery, terrorism or any other form of violence against ships crews, passengers, port facilities, offshore installations and other targets at sea or coastal areas". However, it is worth highlighting that in reality there is not one port in the world that can be declared completely free of security threats. On the positive side, the International Maritime Organisation (IMO) has established a legal and regulatory framework for international cooperation in an effort to make maritime transport of goods and passengers as secure as possible, including the mandatory implementation of risk management instruments through the International Ship and Port Facility Security (ISPS) Code. Yet, the concrete actions for managing risks and deterrence actions must be in accordance with the national maritime security policy for the respective state.

Undoubtedly, to build an effective national maritime security policy (NMSP), the relevant country must establish a national strategy for maritime security first, which must include the development and implementation of a national maritime security plan (NMSP) to support such strategy and the respective threat deterrence actions; restoring passenger and cargo flow, including container cargo, as soon as possible, in the event of an attack or a disruptive event should be a high priority action. However, this plan must be developed based on a national maritime security assessment (NMSA), which must calculate the residual risk related to security threats such as piracy, armed robbery, terrorism, sabotage, illegal transportation of drugs and weapons or any other violent and illegal act against ports, port facilities, ships, crews, passengers, service providers, offshore installations, and other targets in their territorial sea or in the coastal areas.

It is not a coincidence that the United States of America has already developed and implemented a National Plan to Achieve Maritime Domain Awareness (MDA), which includes near-term and long-term objectives, a required program and resource implications, and recommendations for organizational or policy changes, to support the National Strategy for Maritime Security, as directed by National Security Presidential Directive-41/Homeland Security Presidential Directive-13 (Homeland Security of the United Sates, 2022).

Maritime Domain Awareness (MDA), has been defined as "the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment (of the United States)" by the Maritime Security Policy Coordinating Committee Of The U.S., (2005). This very same definition has been applied by the Centre of Excellence for Operations in Confined and Shallow Waters from the North Atlantic Treaty Organization, from NATO (2013), to describe the concept of Maritime Situational Awareness. Though Nordfjeld Ávila-Zúñiga, A.; Dalaklis, D.; Mejia Jr, M. Q. & Neri (2021), defined Maritime Security Awareness as "the effective understanding of any aspect related to the maritime domain that can affect the security of ports, ports facilities, its stakeholders and users, ships and its crews; along with the territorial sea and international waters, including the marine environment, as the key element for a proactive and efficient response against maritime security threats". These authors emphasised the importance to distinguish between Maritime Security Awareness (MSA) and Maritime Domain Awareness (MDA). The latter concept is wider and includes aspects related to maritime safety, which are commonly excluded in the maritime security discipline; they also highlighted their concerns about this fusion, which might complicate consciousness of security risks and intensify current lack of knowledge about types of security incidents versus safety accidents or the so called safety near-misses.

In any case, it is crucial to separate maritime safety issues from maritime security in the maritime and port security national strategy and respective plan. Kenneth (2009), correctly pointed out that "the evolution of organized security processes in the maritime sector can be understood as a product of increasing governmental and commercial concerns about the criminal exploitation of seaports, [...] and the rising threat of global terrorism", while Rudner (2009), included maritime ports as part of the "Critical National Infrastructure" and highlighted the need for a national security and strategy plan for the protection of Canada's critical national infrastructure against exogenous risks and threats.

This paper presents a proposal of a mathematical dynamic model that can be used to calculate the residual risk for the whole country and each of its ports regarding maritime security in real time, by adapting and expanding the formula and procedures established in the ISPS Code to develop a national maritime security assessment, which then shall be basis for the respective national maritime security plan, allowing national authorities to improve maritime situational awareness and adapt to security changes through a better planning of human, economic and material resources to deter maritime security threats.

It is structured in the linear form of introduction, followed by a brief explanation of the ISPS Code, including the PFSA and respectively the PFSP, as well as cyber-security and moving next into an explanation of the methodology used and the presentation of the results. Then, the general discussion is presented, along with the associated conclusions and recommendations. Last but not least, future research directions are provided, including theoretical and practical implications for researchers and practitioners in the areas of maritime security.

2. Maritime Security and the ISPS Code.

To enable economic stability and commerce, it is necessary to protect the free flow of goods shipped by sea (Council of the European Union, 2014; MNE 7,2012; Secretary of Defense USA., 2012; Swedish Maritime Administration, 2014; Till, 2009). The shipping system is composed of many autonomous, but interconnected, actors (Swedish Maritime Administration, 2012) ranging from small local ship owners to large international ship operators.

Maritime security is addressed at many levels, from international bodies such as the United Nations (UN) and the International Maritime Organization (IMO) to single ship operators, but also by both military and civilian organizations. These levels and organizations are interconnected and a security decision

made by one will affect the others (Liwång et al., 2015; Swedish Maritime Administration, 2012).

The ISPS Code strictly corresponds to Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS), 1974 [12] [13] which establishes special measures to enhance maritime security. It is "the comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States", as defined by the IMO (International Maritime Organization, 2012). It is divided in two sections, part A establishes the mandatory provisions, while the non-mandatory ("recommended") part B provides guidelines about how to comply with the obligatory requirements of part A.

Under the ISPS Code, "Contracting Governments may identify a Designated Authority within Government to undertake their security duties relating to port facilities as set out in chapter XI-2 or part A of (the) Code" (International Maritime Organization, 2002b). These maritime security duties and responsibilities include ensuring compliance with the maritime security measures at all ports (where the ISPS Code applies), approval of the Port Security Assessment (PSA) and Port Facility Security Assessment (PFSA), as well as the revision, approval and control of compliance of the Port Security Plan (PSP) and Port Facility Security Plan (PFSP). The PSP/PFSP shall be based upon the PSA and the PFSA, managing all security risk related to the port/port facility and analyses for risk mitigation through the PSA/PFSA, among others (Nordfjeld Ávila-Zúñiga, A.; Dalaklis, 2017).

Under this regulation, the Designated Authority must verify that port and port-terminal operators (port facilities) hire properly certified Port Security Officer (PSO) and Port Facility Security Officer (PFSO) to develop the PSA/PFSA and respective PSP/PFSP, which shall be revised, amended if necessary and approved by the Designated Authority upon implementation. "Once PSP/PFSP are implemented, the designated authority is also responsible for conducting inspection to confirm that all requirements and measures established in the plan are implemented at the respective facility. Then and only then, the Designated Authority may issue the respective Statement of Compliance (SoC), which shall not exceed a period of five years" (Nordfjeld Ávila-Zúñiga, 2018). The responsible person for the continual compliance of the PSP/PFSP is the Port Security Officer (PSO) or Port Facility Security Officer (PFSO), including all requirements established in the ISPS Code and reflected in the PSP/PFSP as training and certification, exercises, practices, inspections audits and modifications via formalised procedures to the plan. In addition, they must attend and respond to security incidents and keep incident security records updated, which must be considered in the risk evaluation and integrated into the security plan to achieve a constant reduction of risks and the continuous improvement of port and maritime security (Nordfjeld Ávila-Zúñiga, A.; Dalaklis, 2017).

According to the IMO, there are certain types of security incidents that are considered serious and must be immediately reported to the Designated Authority and considered for an update of the PFSA/PFSP. These include the following:

- Terror attacks,
- Bomb warnings,
- Hijack,
- Armed robbery against a ship,
- Discovery of other weapons,
- Discovery of explosives,
- Unauthorized access to a restricted area,
- Unauthorized access to the port facility (International Maritime Organization, 2012).

The IMO established three different security levels through SOLAS Chapter XI-2 and the ISPS Code: Security Level 1 (normal) requires the minimum protective security measures at all times. Security Level 2, which requires additional protective security measures for the specific period of time that the risk of a security incident is present and; Security Level 3, which requires high specific protective security measures and may imply the suspension of commercial operations. Security response under Level 3 is transferred to the Government or other organizations responsible for dealing with significant incidents, as explained by the International Maritime Organization (International Maritime Organization, 2002a; 2012) as cited by (Nordfjeld Ávila-Zúñiga, 2018).

According to the research by Cedergren, A. & Tehler (2014), there is, in risk governance, a need to take into account the ways in which risk-related decision-making is performed in settings where many stakeholders are involved, and where these different stakeholders may hold diverse meanings of the concept of central concepts such as risk (Rasmussen, 1985). Therefore, diverse aspects related to maritime security risk governance, such as those indicated by Cedergren & Tehler (2014) and exemplified in Figure 1 below, must be considered in to the NMSA and respective NMSP.

To understand maritime security challenges, it is necessary to define plausible, relevant and challenging threats and scenarios. Qualitative aspects to consider when choosing scenarios include that there should be multiple scenarios to account for uncertainty and each scenario must be plausible, internally consistent, relevant, and contribute to the analysis (Liwång, 2015).

The existing research in maritime security is limited. However research, such as Bichou (2008); (Liwång, H.; Ringsberg, J. W. & Norsell, M. 2013); Liwång, H.; Ringsberg (2013) and (Psarros , et al. (2011), show that empiric data on the shipping system as well as on specific incidents is needed to be able to discuss measures and risk control options. It is also clear from the previous research on society protection in general, such as Cedergren & Tehler (2014), and on maritime security specifically, such as Schneider (2012), that measures are needed on several different levels of the system (Cordner, 2014).

Figure 1: Example: maritime security risk governance in the littoral and at open sea, three conceptual levels of abstraction and four typical stakeholder levels. developed from a generic description of the Swedish risk and vulnerability assessment system by Cedergren & Tehler (2014) and the hierarchical knowledge representation.

Stakeholder levels / Levels of abstraction	**Ships at sea**	**Installations at sea**	**National security enforcing agencies**	**Responsible government control agencies**	**International maritime security framework**
Purpose	Safeguard crew and operation	Safeguard the installations	Work for reducing security risks	National overview of risk	International overview of risk.
Function	Ship security management	Security management	Fight crime and provide for a maritime picture	National risk identification	International risk identification
Form	Implementation of risk controls based on a risk analysis	Unclear	Controls, surveillance and information sharing	Risk assessment and control of security plans	International maritime security codes

Source: Rasmussen, 1985.

3. The Port Facility Security Assessment (PFSA).

The PSA/PFSA is a risk assessment of security threats related to the port or port facility. It includes an analysis of its vulnerabilities and security measures to mitigate such risks, and it forms the basis for the development and updating of the PSP/PFSP. Nordfjeld Ávila-Zúñiga, (2018), explained that among the maritime security measures established by the IMO is the requirement of a periodical revision/update and improvement of PSA/PFSA taking into consideration changes in security threats, changes in the port facility operations, infrastructure or other relevant subjects and after security incidents. The Designated Authority shall also determine the frequency for review of approved PSA/PFSA, while common practice is to review them once a year and in the case of some of the following events: "a) significant security incident at the port/port facility; b) change in the shipping operations undertaken at the facility; and or c) change of facility owner or operator" (International Maritime Organization, 2012).

The IMO establishes certain requirements for the development of PSA/PFSA that include the following elements:

1. Identification and evaluation of important assets and infrastructure;
2. Identification of possible threats to them and the likelihood of their occurrence;
3. Identification, selection and privatization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerabilities; and
4. Identification of weaknesses, including human factors, in the infrastructure, policies and procedures" (International Maritime Organization, 2012).

The PSA/PFSA is built on a six phase assessment:

- Pre-assessment
- Threat assessment
- Impact assessment
- Vulnerability assessment
- Risk scoring
- Risk management

Likewise, with the objective of establishing a standardised method worldwide and considering security measures at a minimum level, the IMO recommends the following formula to score the risk accurately:

RISK = THREAT x IMPACT x VULNERABILITY

However, contracting governments to the SOLAS 1974 Convention are free to demand stricter regulations and requirements for higher security measures than those established by the IMO (which are considered to a minimum level).

In their previous study, Nordfjeld Ávila-Zúñiga (2018), explained that "the method suggested by the IMO assigns a score for the different threat scenarios considering its likelihood of occurrence if there is/was not security measures or score 1 to improbable; score 2 to unlikely; score 3 to likely; and score 4 to probable. Concerning the impact, again allocated on specific criteria, the scores are the following: score 1 to minor; 2 to moderate; 3 to significant and; 4 to substantial. For the assessment of vulnerabilities, targets, strengths, weaknesses, predictability and vulnerability, among other aspects, are included in the analysis where factors as countermeasures and mitigating controls are highly considered, transforming the vulnerability assessment into a vulnerability score. The IMO suggest the following subjective method to allocate a score to vulnerability regarding the extent of risk management: score 1 to robust and effective, (for the case where a complete set of countermeasures is implemented); score 2 to acceptable, (for the case where sufficient countermeasures are implemented to reduce the threat or security risk to an acceptable level); score 3 to limited, (for the case where some countermeasures are implemented and); 4 to none (for the case where none countermeasures or mitigating controls are implemented)".

An imaginary example based on this formula can be developed for the Port of Coatzacoalcos, Mexico, in the Gulf of Mexico: This has been allocated with a Threat Score 3 (considering the illegal activities of drug organizations, oil theft, piratical attacks and organized crime in the area). Then it would be allocated an Impact Score of 4 (considering the critical infrastructure for the energy sector) and a vulnerability of 3 (considering that some security measures and mitigating controls are implemented to prevent the occurrence of security incidents to certain extent but not to an acceptable level). Then, the Residual Risk Score would be 36, equal to 3x4x3.

After common practice, the Residual Risk is classified into three different categories: "high for a Residual Risk Score of 27 and above; medium for a Residual Risk Score of 8-24 and; low for a Residual Risk Score of 6 or less" (International Maritime Organization, 2012). "Threats, impact and vulnerabilities are carefully analysed during the development of the PSA/PFSA, in which must also be included the evaluation of necessary security measures and mitigating controls to reduce the risk to an acceptable level on a sustainable long term bases. If the result of a PSA/PFSA is a high Risk Residual Score it shall be evaluated to include further security measures and stricter mitigating controls; while in the case of a medium Residual Risk Score, the risk and/or threats shall be monitored continuously. For the case of a low Residual Risk Score, there is no need for further security measures" (Nordfjeld Ávila-Zúñiga, 2018).

4. Cybersecurity threats & the PFSA.

Cybersecurity within the maritime context is not limited to prevent cyber-attacks or stopping hackers from gaining access to the operational and information systems, but it also includes protection of digital assets and data, to ensure the continuity of global trade, while ensuring that the maritime industry has the capacity to avert external and internal cyber-security-threats.

Maritime cybersecurity has been defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to protect maritime organizations, their vessels, and their cyber environment by Missionsecure (2022). According to the IMO (2022), maritime cyber risk refers to "a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised".

Operational Technology (OT) and Information Technology (IT) are quite different regarding attack outcomes. Missionsecure (2022), explained that an attack on IT could lead to data theft, while an attack on OT could lead to injury or loss of life, asset damage, or environmental impact. The authors raised concerns about "traditional cybersecurity measures that fail to protect vessels from cyber-attacks and leave the OT network exposed, falling short on providing the visibility and protection required for cyber-physical processes underlying in the maritime industry". The authors highlighted that the complexities associated with vessels and tankers make them vulnerable to high-impact attacks that could last for weeks and spread malware to sister vessels via the corporate network. They previsedthat some of the potential attacks that can cripple a vessel's operations include the following:

- An attack on an OEM network or third-party supplier that spreads to their client's on-vessel OT network,
- An attack on a satellite provider that gains access to a vessel's IT/OT network,
- Exploited cyber vulnerabilities that grant access to a vessel's OT network and provide various attack options, including:
  - GPS/navigation system attack
  - Open/close critical valves
  - Propulsion and rudder control
  - Ballast control
  - Ransomware/Malware
  - Gain full administrative privileges Missionsecure - (2022).

The IMO Maritime Safety Committee (MSC) adopted Resolution MSC.428(98) on Maritime Cyber Risk Management in

Safety Management Systems in June 2017 (International Maritime Organization, 2017). The resolution states that an approved safety management system should include cyber risk management in accordance with the objectives and requirements of the ISM Code, no later than the first annual verification of a company's Document of Compliance after 1 January 2021. From 2021, ship-owners and operators must incorporate cyber risk into ships' safety management systems and appoint a Cyber Security Officer (CySO) on board all ships that shall develop the Cyber Security Assessment (CSA) and the respective Cyber Security Plan (CSP), which is part of the Ship Security Plan (SSP), developed by the Ship Security Officer (International Maritime Organization, 2017). Cyber-security risks must also be considered in the PFSA.

5. Research Methodology.

The research methodology of the current study is focused on adapting the standardised method worldwide, recommended by the IMO to score the risk accurately and included into the International Ship and Port Facility Security Code (ISPS Code), which is the following: RISK = THREAT x IMPACT x VULNERABILITY

This study proposes to adapt and expand this formula to include all ports from a respective country, which along with the necessary programming application can then calculate in real time the total residual risk for all ports of the selected country, provided that the security level is properly updated at all times. The suggested mathematic model is the following:

$$R = \frac{1}{|S|} \sum_{x \in S} T_x I_x V_x$$

It is necessary to clarify that in the suggested model the variables are as follows; R means the total residual risk for the country, while T correspond to Threats, I to Impact and V to vulnerabilities, while S is the set of ports. Based on this equation, a relevant information technology program was created by allocating a variable for each of these factors at each of the ports, at each of the "imaginary encoded" countries, due to the fact that information related to threats, impacts and vulnerabilities at ports is commonly classified as highly confidential.

The programme was created and tested with the possibility to add as many countries as desired and include as many ports in each of the countries as necessary and then, as many port terminals at each port as needed. For testing purposes, a number of five countries was used; each of them associated with three ports and three respective port facilities/port terminals.

6. Results.

The results for the five "imaginary" countries are presented in the figures below. Figure 2 indicates the total residual risk for each of them (A, B, C, D and E) under the column called "average", which is the median for the risk of the associated ports (Port 1, Port 2 and Port 3). These numbers at a country level are also presented in Figure 3, in pie chart format to see it from a general risk comparative perspective. As mentioned before, the programme was developed and tested with the possibility to add as many countries as desired and as many ports in each of the countries as necessary and then, as many port terminals at each port as needed. However, for testing purposes, the number of countries was limited to five with three ports and three respective port facilities/port terminals for each of them.

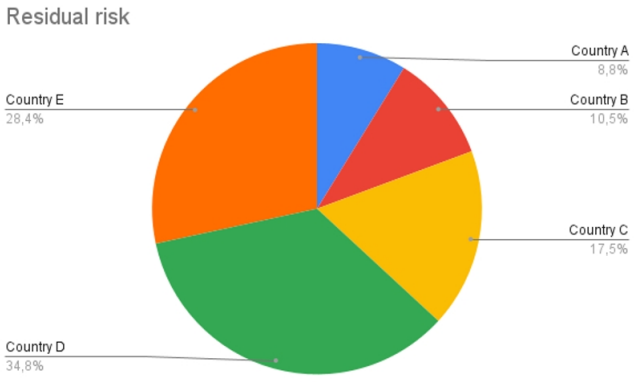
Figure 2: Residual Risk for countries maritime security.

Back | Add country

	Port 1	Port 2	Port 3	Average
Country A	7.5	4.4	2.1	4.7
Country B	11.9	2.9	2.0	5.6
Country C	13.7	7.4	6.8	9.3
Country D	11.3	12.3	32.0	18.5
Country E	15.0	29.3	1.0	15.1

Source: Authors.

Figure 3: Residual risk for countries represented in percent.



Source: Authors.

Figure 2 shows the part of risk for each country in percent, in a scenario where the world is represented with only five countries. The figure 2 and 3 presenting the residual risk for country-level is followed by figures 4, 5, 6, 7 and 8, in which by allocating an "imaginary" value to variables T (Threats), I (Impact) and N (vulnerabilities) for the respective terminal (Terminal1, Terminal 2 and Terminal 3), it is possible to calculate the residual risk for the respective facilities, which then are used to calculate the residual risk for the whole port (Port 1, Port 2 and Port 3).

As mentioned before, the Residual Risk is classified into three different categories: "high for a Residual Risk Score of 27 and above; medium for a Residual Risk Score of 8-24 and; low for a Residual Risk Score of 6 or less" (International Maritime Organization, 2012). Thus, in our model we used the red colour to illustrate countries, ports and terminals with a high residual

risk, yellow to demonstrate medium and green for a low level.

Figure 4: Residual Risk for Ports and terminals of Country A.

Back | Add port

	Terminal 1	Terminal 2	Terminal 3	Average
Port 1	0.4	21.3	0.8	7.5
Port 2	3.4	9.7	0.0	4.4
Port 3	0.0	0.7	5.5	2.1

Source: Authors.

Figure 5: Residual Risk for Ports and Terminals of Country B.

Back | Add port

	Terminal 1	Terminal 2	Terminal 3	Average
Port 1	22.7	12.7	0.3	11.9
Port 2	1.4	1.8	5.6	2.9
Port 3	1.4	4.4	0.1	2.0

Source: Authors.

Figure 6: Residual Risk for Ports and Terminals of Country C.

Back | Add port

	Terminal 1	Terminal 2	Terminal 3	Average
Port 1	18.7	11.9	10.5	13.7
Port 2	7.2	4.1	10.8	7.4
Port 3	9.8	10.5	0.1	6.8

Source: Authors.

Figure 7: Residual Risk for Ports and Terminals of Country D.

Back | Add port

	Terminal 1	Terminal 2	Terminal 3	Average
Port 1	1.0	1.0	32.0	11.3
Port 2	1.0	18.0	18.0	12.3
Port 3	48.0	24.0	24.0	32.0

Source: Authors.

Figure 8: Residual Risk for Ports and Terminals of Country E.

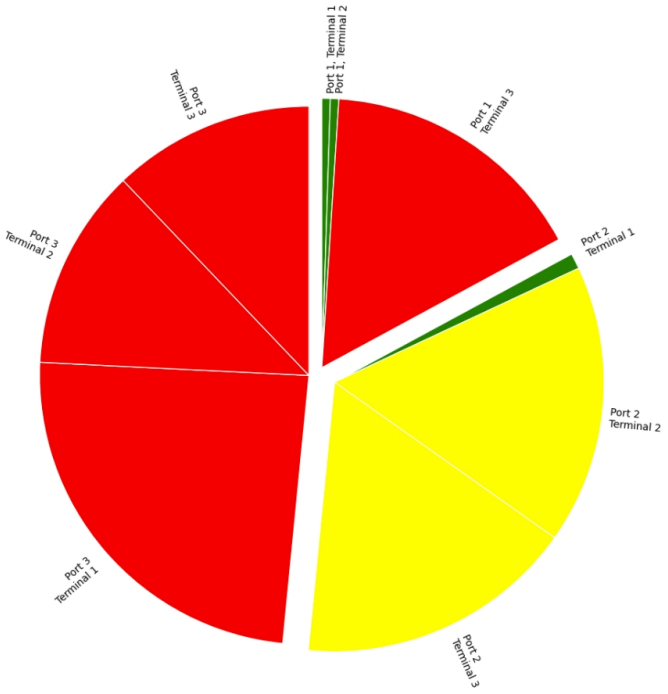
Back | Add port

	Terminal 1	Terminal 2	Terminal 3	Average
Port 1	12.0	24.0	9.0	15.0
Port 2	36.0	36.0	16.0	29.3
Port 3	1.0	1.0	1.0	1.0

Source: Authors.

As explained before, this model provides an overview of the residual risk both at national level and at each port, which would allow the concerned authorities to improve situational awareness adapting to security changes through a better planning of human, economic and material resources to deter maritime security threats. For example, in the case of A and B, the aspects and countermeasures established in ports 2 and 3 (which have a really low risk level), respectively should be assessed to evaluate if some human and material resources as sea patrols could be moved to port 1 to reduce the risk from medium to low level. Another example is country E, where resources for countermeasures in port 3, with a residual risk of 1 should be evaluated for rotation to port 2, which reports a quite high risk with significant security threats. Likewise country D, where Port 3 presents a very high residual risk level (with three terminals in red, figure 9 below) countermeasures should urgently be implemented.

Figure 9: Risk analysis for country D in pie chart.



Source: Authors.

7. Discussing the Swedish Perspective.

Sweden is here used an example of the role of Residual Risk for maritime security could play in the maritime security risk governance for a nation.

In Sweden, the public debate regarding maritime security has mostly been limited to piracy off Somalia and legal aspects of armed guards on ships, two issues with little relevance for maritime security in European waters. However, outside the public eye there have also been specific studies, analyses and exercises initiated by Swedish government agencies such as the Swedish Maritime Administration (Swedish Maritime Administration, 2006), the Swedish Radiation Safety Authority (the exercise Pilot 2015) and the Swedish Armed Forces (a staff exercise regarding maritime security 2016) and academic studies (see for example University of Helsinki, 2009).

These exercises typically deal with a single terrorist attack against a ship under the Swedish flag and includes several organizations and government agencies. However, it does not represent a complete maritime security system perspective based on the nation's maritime strategic security needs.

Moreover, to reduce the identified challenges there is a need for a systems approach that examines different aspects and levels of the maritime security system and how the system delivers utility to a nation or region. A nation's maritime administration has a central role to play and to fully comply this role it is necessary that they have a clear national maritime security strategy, according to a national maritime security assessment, followed by a national maritime security plan, since also other stake holders take decisions that greatly affect maritime security. Such stake holders include ship operators as well as law enforcement agencies that both lack a system level knowledge. This aspect presents specific challenges for the region, nation, and organization responsible for ensuring sufficient maritime security. It also means that the focus is on a nation's (or set of nations and nations' international cooperation) capabilities and efforts needed.

Several Swedish studies have indicated a need for strengthening national transport coordination in response to crises, both as a result of a disruption of the transport system itself (Mötesplats Transporter, 2009; Samverkansområdet Transporter, 2007; Swedish Civil Contingencies Agency, 2014; Swedish Maritime Administration, 2012), but also to avoid that a crisis in other areas and sectors affect the transport system (Samverkansområdet Transporter 2007; Swedish Civil Contingencies Agency, 2014; Swedish Maritime Administration, 2013 and 2014). However, specific Swedish efforts for maritime security are hard to identify.

Previously to this study, the authors intended to develop an analysis over the current status of maritime security in Sweden. Public official and updated maritime security incident statistics is not readily available. Several institutions were contacted to collect data, finding at first glance that there is a significant lack of awareness and knowledge about types of security incidents versus safety accidents or the so-called safety near-misses. Therefore, there is very little evidence of that, and how, the Swedish government agencies implement and enforce maritime security (other than administrative tasks in relation to the ISPS Code) according to Figure 1.

Maritime security threats such as the following, among others, must be considered for the case of Sweden:

1. Transnational organized crime on board ferry traffic between Sweden and Finland
2. Weapons smuggling from the Baltic
3. Drug smuggling from the Baltic
4. Fishing disputes
5. Violation of Swedish waters

Given today's agency structure and responsibility, a risk governance approach is needed and the maritime security efforts need to be further developed and coordinated. Such coordination could efficiently by achieved through a national maritime security assessment (NMSA) and the respective development of a national maritime security plan (NMSP).

Only with a systematic description and understanding of the maritime security system as a whole and at a national level can the performance of the different stakeholders be assessed in relation to their duties and coordination of response to a serious maritime security threat. Therefore, there is a need for an enhanced knowledge on how different stakeholders can strengthen the maritime security system establishing clear duties and responsibilities, including information sharing in the NMSP, which must consider all threat scenarios and deterrence actions evaluated in the NMSA.

Conclusions and recommendations.

1. As a result of the risk-based approach of ISPS Code implementation and enforcement applied at port facility and ship level, it would be extremely beneficial to further develop it to a countrywide level by applying a national and holistic approach to improve not only the assessment of security risks but also manage human, economic and material resources in relation to the identified maritime security threats.
2. The mathematical dynamic model proposed in this paper can provide an effective tool to administer maritime security at the national level, since it calculates in real time the residual risk for the whole country and each of its ports by adapting and expanding the formula and procedures established in the ISPS Code.
3. Due to the fact that the ISPS Code and related instruments have already been implemented by contracting governments to the SOLAS 1974 Convention at all their maritime ports (on the minimum on those that serve international trade needs), the proposed model could facilitate the use of this quantitative solution to administer maritime security risks on a national basis and build the consequent national maritime security plan, which would allow the national authorities to improve situational awareness and adapt to security changes through a better planning.

4. The implementation of this model along with the necessary programming application is recommended as very suitable to manage maritime security at a national level, considering that this methodology is relatively easy to implement and it could considerably strengthen robustness in maritime and national security.
5. An extended version of this model could also be used by the IMO – perhaps through its Global Integrated Shipping Information System (GISIS) – as a way to keep an overview of the general risk at each of its member states (running the model at a country level), assuming that states share with IMO their NMSA and keep these updated at all times.

Future research direction and recommendations.

Future research directions could include the adaptation, development and implementation of the ISPS Code procedures to cover critical infrastructure inland to expand this national maritime security assessment to a general national security assessment.

References.

Bichou, K. (2008). Security and risk-based models in shipping and ports: review and critical analysis. Issue Joint Transport Research Centre Discussion Paper, 20.

Cedergren, A.; Tehler, H. (2014). Studying risk governance using a design perspective. Safety Science, 68(0), 89–98. https://doi.org/10.1016/j.ssci.2014.03.006.

Centre of Excellence for Operations in Confined and Shallow Waters North Atlantic Treaty Organization. (2013). Maritime Situational Awareness. https://www.coecsw.org/our-work-/projects/maritime-situational-awareness/.

Cordner, L. (2014). Risk managing maritime security in the Indian Ocean Region. Journal of the Indian Ocean Region, 10(1), 46–66. https://doi.org/10.1080/19480881.2014.882148.

Council of the European Union. (2014). European Union maritime security strategy (11205/14) (24 June 20).

Homeland Security of the United Sates. (2022). National Strategy for Maritime Security. https://www.dhs.gov/national-plan-achieve-maritime-domain-awareness.

International Maritime Organization. (2002a). Amendments to the Annex to the International Convention for the Safety of Life at Sea, 1974, as Amended. SOLAS/CONF.5/32 ANNEX 2002a.

International Maritime Organization. (2002b). Conference Resolution 2 (adopted on 12 December 2002) Adoption of the International Code for the Security of Ships and Port Facilities. SOLAS/CONF.5/34 ANNEX 1. 2002 b.

International Maritime Organization. (2012). Guide to maritime security and the ISPS Code. International Maritime Organization.International Maritime Organization. (2017). Resolution MSC.428(98) (adopted on 16 June 2017) Maritime Cyber Risk Management In Safety Management Systems. https://www-.cdn.imo.org/localresources/en/OurWork/Security/Documents/-Resolution MSC.428(98).pdf.

International Maritime Organization. (2022). Maritime cyber risk. https://www.imo.org/en/OurWork/Security/Pages/Cybersecurity.aspx.

Kenneth, C. (2009). Port security management. CRC Press Taylor & Francis Group.Liwång, H.; Ringsberg, J. W.; Norsell, M. (2013). Quantitative risk analysis - Ship security analysis for effective risk control options. Safety Science, 58, 98–112. https://doi.org/https://doi.org/10.1016/j.ssci.2013.04.003, 98–112. doi:https://doi.org/10.1016/j.ssci.2013.04.003.

Liwång, H.; Ringsberg, J. W. (2013). Ship security analysis - The effect of ship speed and effective lookout. Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering - OMAE, 2 A. https://doi.org/doi:10.1115/OMAE-2013-10166.

Liwång, H.; Sörenson, K.; Österman, C. (2015). Ship security challenges in high-risk areas: manageable or insurmountable? WMU Journal of Maritime Affairs, 14(2), 201–217.

Liwång, H. (2015). Risk-based ship security analysis – a decision-support approach. Chalmers University of Technology.

Maritime Security Policy Coordinating Committee Of The U.S. (2005). National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security. https://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf.

Mejia, M. (2007). Law and Ergonomics in Maritime Security. Department of Design Sciences, Lund University.

Missionsecure. (2022). A Comprehensive Guide to Maritime Cybersecurity. https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach

MNE Multinational Experiment 7. (2012). Maritime security regime concept.

Mötesplats Transporter. (2009). Samverkan, samordning & samarbete, Nyckelord för fortsatt arbete [Collaboration, coordination and cooperation, Keywords for continued work].

Nordfjeld Ávila-Zúñiga, A.; Dalaklis, D.; Mejia Jr, M. Q.; Neri, K. (2021). Applying the Legal Provisions of the ISPS Code to Streamline Cooperation between Government Authorities Involved in Maritime Security Duties. In M. Musi (Ed.), An Overview of Transport Law Regulatory Policies: The Search for New Answers to Old Problems and Possible Solutions to the Challenges Posed by Technological Evolution, the Pandemic, and Brexit. Bonomo Editore.

Nordfjeld Ávila-Zúñiga, A.; Dalaklis, D. (2017). Enhancing maritime security in Mexico: Privatization, militarization or a combination of both? In P. Chaumette (Ed.), Economic challenge and new maritime risks management: What blue growth? (pp. 81–101). Gomylex.

Nordfjeld Avila-Zúñiga, A. (2018). Building a National Maritime Security Policy. World Maritime University. WMU Research Report Series. https://commons.wmu.se/phd_dissertations/11/.

Nordfjeld Ávila-Zúñiga, A. . D. D. (2018). Assessing the Need of Implementing ISPS Code instruments to Customs Maritime Units, 2018b. In M. Musi (Ed.), Maritime and Transport Law: Between Legacies of the Past and Modernization (pp. 243–260). Bonomo Editore.

Psarros, G.; Christiansen, A.; Skjong, R.; Gravir, G. (2011). On the success rates of maritime piracy attacks. Journal of Transportation Security, (4, Ed.). https://doi.org/https://doi.org/-10.1007/s12198-011-0073-4.

Rasmussen, J. (1985). The role of hierarchical knowledge representation in decisionmaking and system management. IEEE Transactions on Systems, Man and Cybernetics, 15(2), 234–243.

Rudner, M. (2009). Protecting Canada's critical national infrastructure from terrorism. International Journal, 775–797.

Samverkansområdet Transporter. (2007). Öresundsstudien 2006 [The Øresund study 2006].

Schneider, P. (2012). German maritime security governance: a perspective on the Indian Ocean Region. Journal of the Indian Ocean Region, 2, 142–164. https://doi.org/10.1080/19480881.-2012.730749.

Secretary of Defense USA. (2012). Sustaining U.S. global leadership: Priorities for 21st century defense.

Swedish Civil Contingencies Agency. (2014). Research for a safer society – New knowledge for future challenges MSB's research strategy.

Swedish Maritime Administration. (2006). Risk och sårbarhetsanalys för sjöfartssektorn 2005 [Risk and vulnerability analysis for the shipping sector 2005].

Swedish Maritime Administration. (2012). Risk och sårbarhetsanalys för sjöfartssektorn 2012 [Risk and vulnerability analysis for the shipping sector 2012].

Swedish Maritime Administration. (2013). Årsredovisning 2012 [Year Revision 2012, in Swedish].

Swedish Maritime Administration. (2014). Sjöfartsverkets risk och sårbarhetsanalys 2014 [The Swedish Maritime Administration's risk and vulnerability analysis 2014].

Till, G. (2009). Maintaining good order at sea. In Seapower: a guide for the twenty-first century (Second ed., pp. 286–321). Routledge.

University of Helsinki. (2009). Preventing Terrorism in Maritime Regions - Case Analysis of the Project Poseidon. In & P. V. T. In Hellenberg (Ed.), Aleksanteri Papers. University of Helsinki.