Safety in maritime transport - current status and challenges

Marek Robert[1],

[1]Department of Management and Quality Science, Gdynia Maritime University
Poland

***Abstract*— Maritime transport is a sensitive branch of transportation, characterized by an increasing degree of volatility, unpredictability and complexity of the processes carried out by entities involved in maritime transport. The complex subject-entity structure of maritime transport is exposed to numerous risks, both those that are known and monitored, as well as new ones caused by advances in technology and techniques. The article aims to present the existing risks and ways to deal with them - through national and international regulations. The purpose of the article is to give a comprehensive presentation of the organizations and regulations that are designed to ensure safety in maritime transport - shipping and maritime ports and terminals at the macro level. The study was conducted based on the analysis of scientific literature. In the course of the research it became clear that there are many entities creating security in maritime transport, despite this security policy is consistent, although it poses a huge implementation challenge at the level of companies involved in maritime transport.**

During the course of the research, it became apparent that there are no regulations and policies in the area of countering the threats posed by unmanned surface and underwater vehicles. Such vehicles can be used for both military and civilian purposes. In the civilian area, they can be used by pirates and terrorists who may be interested in destroying critical infrastructure such as ports and marine terminals, offshore wind farms, mining platforms, underwater installations, etc. On the other hand, they may threaten to destroy sea vessels with cargo, which may change transport routes, alter maritime transport and logistics chains and increase their maintenance costs. As a result, it is necessary to create not only regulations but viable methods and techniques to defend against this new threat to global maritime transportation routes

Keywords— Maritime transport, Initiatives and programs, safety regulation, AIS, VTS, ISPS, STCW, ISM, FAL, water drones.

I. INTRODUCTION

In Polish nomenclature, maritime transport is understood as two areas of activity integrated with each other - shipping and seaports. The high level of this integration means that an increase in risk in shipping is transferred to an increase in risk in seaports (including sea terminals) and vice versa. Consequently, achieving maritime transportation security poses serious policy challenges given the international nature of much of this shipping activity. No country in the world has jurisdiction over foreign companies transporting cargo/cargo units by ship until they reach a country's territorial waters. Also, no country has resources large enough to guarantee the security of every container transported to the various ports located around the world. Therefore, many governments and economic associations, e.g., the European Union, the African Union, NATO, the IMO, must respond to the increasing levels of global terrorism and/or piracy by creating initiatives, programs and procedures to ensure the security of maritime shipments. Undoubtedly, a breakthrough in maritime security has occurred with the rise of piracy off the coast of Somalia (Bueger Ch. 2015, pp. 159-164.) The dangers of maritime piracy to international trade have made the maritime dimension of security an important consideration for many governments, as the entire international economy is a beneficiary of global trade carried out by maritime transport (Klimek H., Marek R. 2011).

Security is a term that draws attention to new challenges and mobilizes support for their solution. In the broad scientific literature, maritime security is often shown as a threat, that is, it contributes to specific damage or loss (Galić S. et all., 2014; pp. 186.; Klein N. 2011; Kraska J., Pedrozo R. 2013). In contrast to the "negative" definition of maritime security, it can

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 29, No 2 (2025), pages 8
https://doi.org/10.19192/wsfip.sj2.2025.10
Received: March 2025., Accepted: July 2025,
Published: July 2025.

be considered in positive terms, that is, the design of an acceptable or stable order. With that said, it is difficult to clearly define what acceptable or stable maritime security means. Most often, the positive aspect of maritime security is linked to either the economy or technical and technological progress. The first take raises a fundamental question: how a decline in security will affect maritime trade and the global economy. In the technical-technological attempt to define maritime security, the question arises: in what areas do technical-technological advances contribute to an increase in security and in what areas do they contribute to a decrease. Measures to improve security must be balanced so that they do not negatively affect international trade, while at the same time being effective by coordinating efforts to improve the security of maritime transport. Unfortunately, this is where the additional problem of finding a compromise between the security of maritime transport and its productivity and economic efficiency arises. In other words, a golden mean must be found between security and the economic costs of implementing and maintaining it. Excessively high security costs may contribute to an increase in the cost of shipping and this will contribute to a decline in international or global trade. Also, if, as a result of increased security, there is a decrease in the efficiency of cargo handling at seaports/terminals, this too can contribute to participants in international or global trade looking for alternative shipping routes. We know from modern history that excessively high costs and/or poor cargo/container handling efficiency caused cargo to gravitate to foreign ports instead of domestic ports. The same principle applies to the overregulation of security procedures, programs and initiatives both at the level of a single country and countries jointly implementing various solutions to improve the state of maritime transport security. An additional question that directly relates to maritime transportation security concerns the optimal amount of national or associated country resources to be devoted to maintaining or improving it, how security institutions work, and how much the security policies of a country or association of countries affect the ability of maritime transportation actors and even more broadly of supply chain actors to operate freely in maritime trade and transportation.

"Security," in the context of this study, should be understood as a framework of laws, processes, procedures, programs, initiatives used to protect maritime transport from threats (terrorism, piracy, robbery, theft of cargo and cargo units, trafficking in drugs/people/weapons/prohibited cargo and dual use, theft and data and information crimes, environmental pollution) that can threaten assets (such as cargo, ship, crew and passengers, port and terminals, offshore installations, and data and information). To enhance security, security requirements are being created by both state institutions, international associations and private companies. The latter often impose higher standards for ensuring security than those set by relevant national or international laws. Customers executing commercial contracts of high financial value know that the weakest link in the transportation/logistics chain can lead them to huge financial losses. Therefore, they take measures to ensure that all participants in a commercial contract meet "high" security standards, thus offsetting the possibility of significant financial losses due to failure to meet commercial terms associated with the implementation of highly capital-intensive and complex maritime projects. For these higher security requirements, customers are willing to incur additional costs but, by doing so, they increase the chance of realizing the commercial contract both in terms of the adopted financial budget and its execution time. This means that they are willing to give up above-average profits from a commercial contract but get a lower but reasonably "certain" financial return for it. The great complexity and capacity of the security matter cause that in the following part, the article will focus on security requirements set by international regulations.

II. RESEARCH MANUSCRIPT SECTION

A. Materials and Methods

Various initiatives and programs to increase security in maritime transportation are being undertaken by countries, international organizations and economic blocs. These initiatives address various players in the supply chain, but the greatest emphasis is on shipping companies, ports and marine terminals. Such initiatives and programs are designed to make ongoing analysis, assessment and recommendation of acceptable levels of security for:

- ship/other vessel;
- port/terminal;
- cargo/unit of cargo;
- crew/passengers; and
- the environment.

Currently, a number of procedures, regulations, programs and initiatives are concerned with ensuring the safety of both ships and ports/terminals at sea. For vessels, an important element in improving safety is the Automatic identification System (AIS). The Automatic Identification System is applicable in all maritime waters, which is effective when the vessel has its transponder activated. There are various AIS websites for public use, and it is often the only way for many organizations (for example: logistics operators, shippers, carrier representatives, etc.) to monitor the position of a vessel, including, unfortunately, terrorist organizations and pirates. Captains of commercial vessels, knowing the areas of increased risk of attack by pirates, turn off the transponder, and then the vessel is not visible to the AIS system, and thus to other organizations monitoring and controlling the position of the vessel (Stupak T., 2014).

Another extremely important instrument for improving safety is the EU directives on monitoring and tracking the position of vessels. To this end, various Vessel Traffic System (VTS) systems have been developed to monitor, track, plan, organize and control the movement of ships in seaports . However, there is still no fully integrated VTS system for all seaports operating worldwide, and as a result, seaport managers have their own system solutions related to vessel traffic control. The European Union's seaport authorities and those located outside the European Union, for various reasons, do not provide information to other ports on vessel traffic, and as a result, there is no way to fully monitor and control seagoing vessels (Marek R., 2016, pp. 222-228).

As a result of the increasingly sophisticated systems used on ships and the increasing number and size of vessels, means that an important element of security is the training of floating crews so that they can ensure the safety of the vessel, the security of port facilities/terminals, the cargo being carried and the protection of passengers. To this end, minimum training requirements are set for all personnel serving on vessels. These requirements include personal survival techniques; fire prevention and firefighting; medical first aid; marine hazard awareness; communication; leadership; teamwork and human behaviour. Crew training requirements become important when providing protection for passengers on cruise and passenger ships. This means that employees must be additionally trained in crowd management skills and passenger care to ensure real security and not just a sense of it. This type of extensive safety is provided through a system of training enforced by the STCW (International Convention on Standards of Training, Certification and Watchkeeping) Convention. (International Maritime Organization, 2001). The responsibility for training the ship's crew rests with shipping companies.

With regard to the terrorist act that took place in the United States on September 11, 2002, multilateral regulations were created at the initiative of the United States, which initiated new maritime security requirements. In December 2002, the International Maritime Organization developed The International Ship and Port Facility Security Code (ISPS) and added it as an amendment to the International Convention for the Safety of Life at Sea (SOLAS) (Talaie F., Javidbakht M., 2021, pp. 119-149). The code sets out mandatory security requirements that governments, ports, terminal operators and shipping companies must meet in order to enhance the safety of the global maritime transportation system. In the case of the ISPS Code, compliance with all rules is enforced by the responsible national government agency, and violations are dealt with by the relevant maritime authorities at the national level. The IMO does not publish any blacklist, so the ISPS safety system is only effective if national flag regulations are respected and shipping lines and seaports meet the safety requirements set.

Important regulations for improving safety are the ISM (The International Standard for the Safe Management and Operation of Ships and for Pollution Prevention.) Code, which aims to, improve maritime safety, prevent pollution, promote safety culture, create safety management standards, enhance safety competence, improve maritime safety, improve emergency preparedness, promote continuous improvement, facilitate flag state control. Its main tools are procedures, instructions, schedules and checklists. The ISM Code applies to virtually all operational activities of maritime transport companies, which must implement them - excluding accounting and finance. All procedures are designed to identify risks (e.g., in the areas of operations, communications, vessel entry or exit from port, bunkering, ship manning, loading, unloading, commercial activities, cargo handling operations, ship crane lifting operations, etc.).

These procedures are reviewed and re-reviewed from time to time. Adverse events occurring in the operations of a maritime transport company that has an ISM code in place are a cause for revisiting the procedure, and improving it in such a way that the adverse event does not have the possibility of happening again. In this way, maritime safety is subjected to a continuous process of improvement and, consequently, its negative effects are minimized. As can be seen. The ISM Code is similar to TQM in terms of the structure of the operation, only it is oriented towards operations in the maritime industry. As a result, it is easier for maritime transport companies to obtain quality certificates (Karahalios H. et all., 2014, pp. 391).

The FAL (Convention on Facilitation of International Maritime Traffic) was created to improve the safety of shipments in terms of formalities, with the main purpose of preventing unnecessary delays in maritime traffic, assisting cooperation between maritime states, and ensuring the highest possible degree of uniformity in terms of paperwork, documentation and other procedures to improve the handling of cargo/containers and vessels (Directive 2002/6/EC of the European Parliament and of the Council of 18 February 2002 on reporting formalities for ships arriving in and/or departing from ports of the Member States of the Community, 2002). This convention specifically addresses the entry and exit of a vessel from a seaport, stores held on board, cargo, and data and information requirements for the vessel's crew. The convention aims to ensure the security of data and information passing through various international institutions and to introduce certain standards for its management (Marek R. 2017, pp. 462).

Another important regulation to improve safety in maritime transportation is the International Maritime Dangerous Goods Code. Its regulations, guides, procedures, and guidelines are intended to enhance the safety of the vessel, port/terminal, cargo/unit of cargo, crew, and the environment. The regulations do not directly mention environmental protection, but by properly applying the provisions of this convention, the environment becomes safe.

In order to enhance the security of international and global cargo trade, the United States has implemented advance notification policies and launched a number of programs, including:

- container security initiative (CSI),
- Customs-Trade Partnership Against Terrorism (C-TPAT),
- importer security document (ISF), under the “10+2” program.

The Container Security Initiative, on the other hand, focuses on ensuring the safe movement of containers within the container logistics chain passing through sea and ocean routes. The initiative is a bilateral agreement between the U.S. and other countries, under which the U.S. places its customs officials at foreign ports as part of the pre-screening process and the ability to pre-inspect containers according to U.S. standards at foreign ports, thus moving its customs border overseas. As of January 01, 2023, 26 countries and 44 ports were participating in CSI (Widdowson D., Holloway S. 2009).

Another important program of interest to cargo owners is C-

TPAT, which is by no means the only one affecting the movement and processing of goods in international trade. The goal of the Customs-Trade Partnership Against Terrorism C-TPAT program is to make security a common activity throughout the cargo supply chain (Laden, Michael D., 2007, pp. 75-80). The program seeks partnerships between the U.S. government and domestic and foreign companies, and aims to protect maritime supply chains from harbouring terrorist weapons, contraband and other items that threaten the security of the United States.

This initiative turned into a program is designed to protect the United States from various defined threats under C-TPAT, and its costs are passed on to all participants in the entire supply chain that export their material goods to the US. This means all participants in the chain, that is: foreign manufacturers, suppliers, suppliers' vendors, contractors and subcontractors, warehouse providers, as well as air, sea and land carriers must adhere to specific recommendations including: physical security, access controls, procedural security, personnel security manifest procedures, conveyance security, and education and training awareness (Banomyong R., 2005, pp. 3–13).

Another initiative to enhance security is the Proliferation Security Initiative (PSI). The initiative aims to stop the illicit trafficking of weapons of mass destruction, the systems that carry them and related materials. The Anti-Proliferation Security Initiative was proposed by the USA in Krakow (Poland) (Koch S.J., 2012, pp. 8-10) and currently brings together 101 countries (Proliferation security initiative· 2023).

An additional form of security assurance in the cargo area is The Importer Security Filing (ISF), also referred to as the “10+2” program (Tirschwell P., 2009). The ISF is a customs import requirement set by U.S. Customs and Border Protection; which requires that, for security reasons, container cargo information must be provided to the agency at least 24 hours before the vessel enters a seaport. This rule applies to imported cargo arriving in the United States by ship. Failure to comply with the rule could ultimately result in fines, increased inspections and cargo delays. The program imposes obligations on the importer and the carrier to provide data and information on the cargo, the cargo unit and the vessel, and the parties to the transaction.

Another solution to ensure safety in maritime transportation is Ports 24 hours. Ports 24 aims to improve service and speed up cargo clearance at seaports. Some imported goods, especially food, are subject to various inspections, i.e. Customs Service, Veterinary Inspection, State Sanitary Inspection, Agricultural and Food Quality Inspection and State Plant and Seed Protection Inspection (Florczyk R.A., 2015, pp. 14-15). Each of these services is authorized to carry out independent, autonomous inspection activities. As a result, the same shipment could be inspected several times by different institutions. The Customs Service is tasked with completing all inspections at the maritime border within 24 hours, by coordinating the activities of all the aforementioned controlling inspections. At the same time, the Customs Service is responsible for coordinating inspections at seaports in such a way that they can be carried out by all inspections in the least organizationally burdensome manner for importers and operators. With the exception of the case where it is necessary to carry out laboratory tests or subject the goods to quarantine or, in the case of live animals, isolation, the duration at seaports of inspections of goods imported from third countries, including those carried out by the Customs Service authorities, should not exceed 24 hours, calculated from the moment the goods are presented for inspection, a complete application for inspection is submitted to the competent authorities, and information on the time and place of inspection is provided, to the release of the goods for a customs procedure. Thus, the start of the 24-hour period depends on the combined fulfilment of three prerequisites: the availability of the goods, the completion of the applications, and the appointment of the time and place of inspection. To facilitate this task, information exchange computer systems are being implemented, involving both border inspections and traders. Dedicated information systems for 24-hour customs service to ports allow tracking the current status of cargo activities, annotation in the system eliminates the need to present paper documents. 24-hour ports provide many facilities in the field of: VAT settlement; control facilities for AEO certificate holders, clearance before the ship arrives at the port, smart and secure trade lines; single window service (Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU, 2019); regular shipping service, while maintaining a high level of security for imported cargo (Marek R. 2017, pp. 465).

Another important area for ensuring freight security on the part of cargo is the resolution adopted in 2002 by the Customs Cooperation Council on Security and Disruption of International Trade in Supplies. Since the adoption of this resolution, a World Customs Organization (WCO) Task Force has been established and has developed a package of measures including: improving the WCO's data model and creating a list of necessary data to identify high-risk shipments; defining guidelines for advance information on cargo, creating a system to enable the electronic transmission of customs data prior to the arrival of goods at a seaport (Integrated Supply Chain Management Guidelines); creation of WCO guidelines for customs agents to work with members and private industry to enhance supply chain security and thereby create facilitation of cargo movement in international trade; and an International Convention on Mutual Administrative Assistance in Customs Matters was created to help WCO members develop a legal basis to support WCO initiatives. The goal of the WCO's efforts, from a cargo perspective, was to develop a framework of standards that would encourage trade facilitation in a seamless manner and that could be consistent across customs jurisdictions (World Customs Organization, 2021).

Security is not just about programs and business processes. Traditionally, container seals are proof of the integrity of the cargo with the container, and cargo owners do not regard them as a barrier to thieves, as they are easy to break and “repair” in such a way that it does not raise any suspicion for participants in the container logistics chain and especially customs. Therefore, cargo interests have sought to define appropriate standards to achieve their security goals. Producers of high-value goods have previously taken various initiatives to ensure the security of cargo moved in containers, initially experimenting with tracking equipment using GPS and monitoring the status and quantity of cargo inside the container. Also, there is increasing use of RFID “passive and active” radio frequency identification technology, which is used as part of the management of the inventory contained in the container unit. The problem with RFID technology is that it can be used to illegally track cargo along with a container unit. However, we must also look at the container more broadly, not only from the point of view of ensuring the safety of the cargo in it, but also from the point of view of the security of the critical infrastructure through which the container moves. Unfortunately, a sea container can also be used as a tool of a terrorist act, when the explosive device (or a device of mass destruction) contained in it can be remotely detonated, destroying the infrastructure of a seaport, a maritime container terminal, an inland intermodal terminal or an important production plant to which the container was delivered. In order to increase the safety of cargo movement in a container, an electronic seal has been introduced as a "first-line" solution to increase the safety of cargo transportation in a container (Bichou, K. et all., 2007). However, the biggest problem that interferes with the adopted level of security is the human factor, because the integrity of the cargo with the container does not guarantee that the contents contained in it are consistent with the cargo declaration. Therefore, the most important method to increase the safety of container movement is still the technology of selective but targeted scanning of container contents and its verification based on cargo data contained in the cargo manifest.

An important element of the increase in the level of security are ISO – 28000 and 28001 certificates, which relate to supply chain security management. Certification by an independent third party confirms that your supply chain security management system complies with the requirements of ISO 28000 (United Nations Conference on Trade and Development 2015). In this way, maritime transport entities confirm that they have systems in place to manage and mitigate critical points to ensure the security of the supply chain. The benefits of this certification for maritime transport includes:

- facilitating trade and accelerating the cross-border transport of goods and loaded units;
- improved work efficiency;
- monitoring and managing security threats;
- encouraging maritime companies to secure their own logistics processes;
- enabling maritime management to focus on crucial areas;
- compare safety maritime management practices;
- achieve cost savings by reducing security incidents;
- demonstrate a commitment to the safety of people and the protection of vessel and goods/loaded units.

Energy security is an increasingly important security issue. The main purpose of the ISO 5001 system is defined as “to enable organization to establish the systems and processes necessary to improve energy performance, including energy efficiency use and consumption” (ISO, 2011). The use of ISO 5001 means that the energy management system is intended to help maritime transport companies establish an organizational structure that allows them to focus on energy security by increasing the efficiency of the use of vessels, port facilities and the movement of container units in the maritime transport/supply chain. By implementing these standards, maritime transport companies can develop new methods of monitoring energy consumption, thereby improving their energy security and reducing emissions of various fumes (Buhaug, Ø. et all., 2009) and other pollutants into the natural environment.

Also, safety in maritime transport is implemented by regulations of the International Labour Organization, which is tasked with creating safety in terms of: standards, basic principles and labour rights; creating equal opportunities for men and women in terms of employment conditions, and providing social protection for maritime transport workers (Ryder G., 2015). The International Transport Federation is the guardian of this compliance with this security. At the same time, these regulations are consistent with the provisions of the STCW/IMO Convention. Occupational safety regulations must permanently adapt to changes in the area of automation, autonomous (Mallam, S.C. et all., 2020, pp. 334-345), robotization and digitalization of work at sea and this means improving and raising the necessary competence (Kilpi, V. et all., 2021, pp. 610-626), which must be expressed in the corresponding international regulations.

On the basis of the discussed initiatives, programs, regulations, and procedures, it is possible to list the authorities that actively participate in the creation of maritime safety, through specific methods that affect various participants in the transport and logistics chain, as reflected in Table 1.

TABLE 1: SUMMARY OF METHODS TO IMPROVE SAFETY IN MARITIME TRANSPORT WITH REGARD TO ITS PARTICIPANTS

Organisation	Methods	Year	Vessel	Port/terminal	Cargo/Container Units	Vessel’s crew/passengers	Environment
IMO	SOLAS/DIRECTIVE UE/VTS	2002/59	X	X	X	X	
IMO	SOLAS/AIS	2002	X				
IMO	STCW	1978	X			X	
IMO	SOLAS/ISPS	2002	X				
IMO	SOLAS/MARPOLS/IMDG	1965/2002	X	X	X	X	X

Organisation	Methods	Year	Vessel	Port/terminal	Cargo/Container Units	Vessel's crew/passengers	Environment
IMO	SOLAS	SOLAS 1974	X			X	
IMO	SOLAS / ISM	1994	X	X	X	X	X
IMO	FAL	1967	X	X	X	X	
ISO	28000/ 28001	2005	X	X	X		
ISO	5001	2010/ 2018	X	X			
Bureau of Customs and Border Protection US	CSI	2002	X	X	X	X	
US	PSI	2003	X	X	X		
US Bureau Customs and Border Protection	C-TPAT	2002	X	X	X	X	
U.S. Customs and Border Protection	ISF	2009	X	X	X	X	
World Customs Organisation	Port 24	no data	X	X	X	X	
ONZ/The International Labour Organisation	MLC	2006				X	

Source: own elaboration

Cyber threats are and will be an important problem and challenge in maintaining security in maritime transport. Cybersecurity is the top priority in the maritime transport sector, and the use of breakthrough technologies should not threaten its operational and commercial activities. Nevertheless, maritime transport is a significant target for hackers. Currently, it is difficult to determine how many cyberattacks there are on a global scale against ships, ports and maritime terminals (Raheem A.N.A.R., 2021, pp. 248-255). A cyberattack is an illegal activity that directly affects the operations of ports/marine terminals and shipping lines, their reputation and trust among participants in the maritime transport/logistics chain. In order to ensure security from cyberattacks, it is necessary to be aware of the existence of such attacks (de la Peńa Zarzuelo. I., 2021, pp. 1-4) and to identify new threats and take pre-emptive actions regarding this danger whenever possible.

Unfortunately, there is currently a very turbulent environment, which means that maintaining the adopted level of safety may be difficult, or perhaps impossible, in the near future, as a result of increased progress in the field of technology. The emergence of surface and underwater unmanned vehicles may disrupt the safety of maritime transport. Unmanned water facilities will be used to an increasing extent for military operations by various countries, i.e. they will be used for espionage, provocative activities and warfare. This type of unmanned vehicles means that even countries significantly distant from their enemies can no longer feel safe and must create systems that will enable them to neutralize this type of offensive or military action with the use of drones. In the latter case, the unmanned underwater vehicles will be equipped with explosives, which means an additional danger of pollution for the aquatic environment, as well as for global maritime trade. Unfortunately, maritime drones can be used as a weapon by terrorists or pirates, which can negatively affect the security of maritime supply chains. This means that there will be no need to kidnap crews or seagoing vessels, as has been the case so far, and it is enough to terrorize sea and ocean carriers with the destruction of ships to achieve the same effect. This could have consequences for maritime trade and thus global trade. Such actions may contribute to an increase in freight rates to cover the costs of ransoms paid to terrorists, an increase in insurance prices, expenses related to changes in the route of ships, expenses for the purchase of direct protection equipment against attacks by sea robbers. Owners of offshore wind farms, seaports or wealthy seaside towns – health resorts, living off tourist resources – will also face a similar problem. In order to overcome the upcoming problems with the development of technology enabling the use of surface and underwater unmanned vehicles, it is necessary to create a security system that would neutralize this type of terrorist and military acts and clean fragments of damaged or destroyed naval drones lying on the bottom of various sea and ocean basins.

B. Results and Discussion

Based on the above analysis, various security initiatives, programs, regulations can be said to fulfil their role by bringing various areas of maritime transport (that is, cargo, cargo units, ship, environment), as well as various participants in transport and logistics chains, into the security assessment. Although the importance of initiatives, programs and regulations undoubtedly takes time away from the preparation, maintenance and re-verification of procedures, and generates costs, it contributes to maintaining the adopted level of security at the macro and micro level. Maintaining security in maritime transport at the macro level is carried out by states, blocs of states and international organization. Currently, each country with access to the sea and oceans is creating its maritime security solutions, most often taking into account the requirements including international maritime organizations.

However, it should be noted that the main initiator of safety design in maritime transport is the United States, whose initiatives and programs are applied directly or indirectly through appropriate amendments and changes in other countries or blocs of countries - such as the European Union through regulations and directives. Also, international organizations such as the International Maritime Organization, the International Organization for Standardization, the World Customs Organization, and the International Labour Organization directly shape safety policy in maritime transport. Undoubtedly, safety policies made at different levels (state, bloc of states, international organizations) should be consistent and unambiguous, as they must be implemented at the micro level - by maritime transport companies. And the challenges of implementing security regulations must be dealt with in companies in a consistent and economically sound manner, i.e., maritime transport companies must focus mainly on their operational activities and security must be provided at the adopted level but in such a way that it does not burden the costs of core activities. An interesting question that may arise is how the share of security costs in maritime transport companies affects its return on equity.

The contribution of this study is the inclusion of a comprehensive overview of the various entities responsible for designing the level of security, and their regulatory solutions that must be implemented in maritime transport enterprises. Most of the scientific studies on this issue, focus on the analysis of a selected regulation and its method of implementation in maritime transport enterprises or comparisons between regulations and their methods of improving safety. This study differs from other studies in its comprehensiveness, of course, also limited by the size limitation of this article.

A further contribution of this study is to highlight the problem arising from the use of maritime unmanned underwater and surface vehicles, which unfortunately can be used by terrorists to destroy critical infrastructure - port/terminal, offshore mining platforms, offshore wind farms, pipelines and submarine cables, etc. The article also points out that sea drones can be used by terrorists and sea pirates to destroy or damage sea and ocean vessels, which can result in changes in shipping routes, changes in transportation and logistics chains, and to an increase in the cost of such transportation. In order to address this problem, security regulations and methods should be created to eradicate attacks by unmanned surface and underwater craft.

Maritime safety is not just a slogan, but above all procedures, programs and initiatives that are to ensure the safety of maritime transport, and thus international trade. The different actors involved in maritime transport are subject to different regulations and codes that they must implement and comply with. Participants of maritime transport who participate in the handling of cargo imported to the United States are subject to much more stringent security procedures that they must meet.

However, despite the existence of various system solutions increasing the level of safety in maritime transport, technological progress causes its increasing threat. Undoubtedly, surface and underwater unmanned vehicles pose a huge challenge to ensuring the security of maritime transport, which may be subject to terrorist acts or piracy. In practice, this means that a system must be set up within the seaport, ship and other critical infrastructure.

III. Conclusions:

Based on the above analysis, various security initiatives, programs, regulations can be said to fulfil their role by bringing various areas of maritime transport (that is, cargo, cargo units, ship, environment), as well as various participants in transport and logistics chains, into the security assessment. Although the importance of initiatives, programs and regulations undoubtedly takes time away from the preparation, maintenance and re-verification of procedures, and generates costs, it contributes to maintaining the adopted level of security at the macro and micro level. Maintaining security in maritime transport at the macro level is carried out by states, blocs of states and international organization. Currently, each country with access to the sea and oceans is creating its maritime security solutions, most often taking into account the requirements including international maritime organizations.

However, it should be noted that the main initiator of safety design in maritime transport is the United States, whose initiatives and programs are applied directly or indirectly through appropriate amendments and changes in other countries or blocs of countries - such as the European Union through regulations and directives. Also, international organizations such as the International Maritime Organization, the International Organization for Standardization, the World Customs Organization, and the International Labour Organization directly shape safety policy in maritime transport. Undoubtedly, safety policies made at different levels (state, bloc of states, international organizations) should be consistent and unambiguous, as they must be implemented at the micro level - by maritime transport companies. And the challenges of implementing security regulations must be dealt with in companies in a consistent and economically sound manner, i.e., maritime transport companies must focus mainly on their operational activities and security must be provided at the adopted level but in such a way that it does not burden the costs of core activities. An interesting question that may arise is how the share of security costs in maritime transport companies affects its return on equity.

The contribution of this study is the inclusion of a comprehensive overview of the various entities responsible for designing the level of security, and their regulatory solutions that must be implemented in maritime transport enterprises. Most of the scientific studies on this issue, focus on the analysis of a selected regulation and its method of implementation in maritime transport enterprises or comparisons between regulations and their methods of improving safety. This study differs from other studies in its comprehensiveness, of course, also limited by the size limitation of this article.

A further contribution of this study is to highlight the problem arising from the use of maritime unmanned underwater and surface vehicles, which unfortunately can be used by terrorists to destroy critical infrastructure - port/terminal, offshore mining platforms, offshore wind farms, pipelines and

submarine cables, etc. The article also points out that sea drones can be used by terrorists and sea pirates to destroy or damage sea and ocean vessels, which can result in changes in shipping routes, changes in transportation and logistics chains, and to an increase in the cost of such transportation. In order to address this problem, security regulations and methods should be created to eradicate attacks by unmanned surface and underwater craft.

Maritime safety is not just a slogan, but above all procedures, programs and initiatives that are to ensure the safety of maritime transport, and thus international trade. The different actors involved in maritime transport are subject to different regulations and codes that they must implement and comply with. Participants of maritime transport who participate in the handling of cargo imported to the United States are subject to much more stringent security procedures that they must meet.

However, despite the existence of various system solutions increasing the level of safety in maritime transport, technological progress causes its increasing threat. Undoubtedly, surface and underwater unmanned vehicles pose a huge challenge to ensuring the security of maritime transport, which may be subject to terrorist acts or piracy. In practice, this means that a system must be set up within the seaport, ship and other critical infrastructure.

IV. References

Banomyong R. The impact of port and trade security initiatives on maritime supply-chain management. *Maritime Policy Management*, 2005; Volume 32, pp. 3–13.

Bichou, K.; Bell M. G.H.; Evans A. *Risk management in port operations, logistics and supply chain security –Lloyd's Practical Shipping Guides*, Informa Law, London, 2007.

Bueger Ch. What is maritime security?, *Marine Policy*, 2015; Volume 53, pp. 159-164.

Buhaug, Ø.; Corbett J.; Endresen O.; Eyring V.; Faber J.; Hanayama S.; Lee D.; Lindstad H.; Mjelde A.; Plsson C.; Wanquin W.; Winebrake J.; Yoshida K. *Second IMO greenhouse gas study*. International Maritime Organisation, London, 2009.de la Peńa Zarzuelo. I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy*. 2021; Volume 100, pp. 1-4.

Directive 2002/6/EC of the European Parliament and of the Council of 18 February 2002 on reporting formalities for ships arriving in and/or departing from ports of the Member States of the Community (Text with EEA relevance) Official Journal L 067, 09/03/2002 P. 0031 – 0045, 2002.

Florczyk R.A. Autostrada celna. *Namiary na Handel i Morze*, 2015; pp. 14-15. (Polish Version)

Galić S.; Lušić Z.; Skoko I. The role and importance of safety in maritime transportation. *International Maritime Science Conference,* Book of Proceedings, Cratia, 2014; pp. 186.

International Maritime Organization, *STCW 78*, as amended 1995 and 1997, London, 2021.

ISO. *Energy Management Systems: Requirements with Guidance for Use* (Geneva:ISO). 2011.

Karahalios H.; Yang Z.L.; Wang J. *A risk appraisal system regarding the implementation of maritime regulations by a ship operator. Maritime Policy & Management*, 2014; Volume 3-4, pp. 391.

Kilpi V.; Solakivi T.; Kiiski T. Maritime sector at verge of change: Learning and competence needs in Finnish maritime cluster. *Journal of Maritime Affairs*, 2021; Volume 20. pp. 610-626.

Klein N. *Maritime security and the law of the sea*. Oxford & New York, Oxford University Press, 2011.

Klimek H.; Marek R. Żegluga morska wobec zagrożeń piractwem i terroryzmem. *Studia i Materiały Instytutu Transportu i Handlu Morskiego*, Zeszyty Naukowe Uniwersytetu Gdańskiego, Gdańsk, 2011; pp. 62-69. (Polish version).

Koch S.J. *Proliferation Security Initiative: Origins and Evolution*. National Defense University Press Washington, D.C., 2012; pp. 8-10.

Kraska J.; Pedrozo R. *International maritime security law*. Leiden and Boston, Martinus Nijhoff, 2013.

Laden M. D 'The genesis of the US C-TPAT program: lessons learned and earned by the government and trade'.*World Customs Journal*, 2007; Volume 1, pp. 75-80.

Mallam S.C.; Nazir S.; Sharma A. The Human Element in Future Maritime Operations-Perceived Impact at Autonomous Shipping, *Ergonomics*, 2020; Volume 63, pp. 334-345.

Marek R. A qualitative analysis of using SWIŻB system into creation of Polish Port Community System. *Carpathian Logistics Conference*, Zakopane, 2016; pp. 222-228.

Marek R. The Role and place of Customs in Port Community System – experience from Poland. *17th International Scientific Conference on Business Logistics in Modern Management*, Croatia, 2017; pp. 462.

Proliferation security initiative (2003), available online: https://www.state.gov/proliferation-security-initiative/ (accessed on 15.11.2024).

Raheem A.; Ali N.A.R.; Chebotareva A.A.; Chebotarev V.E. Cyber security in marine transport: opportunities and legal challenges. *Scientific Journal of Maritime Research*, Rijeka 2021; Volume 35, pp. 248-255.

Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU (EMSWe Regulation), 2019.

Ryder G. The International Labour Organization: The next 100 years. *Journal of Industrial Relations*, 2015; Volume 57, pp. 48-757.

Stupak T. Influence of Automatic Identification System on Safety of Navigation at Sea, *TransNav* , Gdynia Maritime University, 2014; Volume 8, pp. 337—341.

Talaie F.; Javidbakht M. Analysis of the ISPS Code and Its Implementation: Case Study of Malaysia and South Korea, *International Journal of Maritime Policy*, 2021; Volume 1 , pp. 119-149.

Tirschwell P. 'The truth about 10+2'. *Journal of Commerce Online,*, 2009, available online: www.joc.com/node/409178., (accessed on 08.12.2024).

United Nations Conference on Trade and Development. *Review of Maritime Transport*, New York and Geneva, 2015; pp. 9.

Widdowson D.; Holloway S. '*Maritime Transport Security Regulation: Policies, Probabilities and Practicalities'*,Workshop 4: Ensuring a Secure Global Transport System, International Transport Forum, Leipzig, Germany, 2009; available online: www.internationaltransportforum.org/2009/forum2009.html. (accessed on 12.12.2024).

World Customs Organization, *WCO SAFE Framework of standards*, WCO, Brussels, 2021; available online: https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/safe-framework-of-standards.pdf, (accessed on 15.12.2024).