DOI: https://doi.org/10.34862/rbm.2020.1.10

Andrzej Bursztyński
Polish Naval Academy of the Heroes of Westerplatte
a.bursztynski@amw.gdynia.pl
https://orcid.org/0000-0002-9590-4680

Safety of Maritime Critical Infrastructure Facilities in the Aspect of Contemporary Threats

Summary: The article attempts to present maritime infrastructure facilities that may or should be included in critical infrastructure facilities. Due to their nature and importance for safety and economy, these facilities may be classified as national or European critical infrastructure facilities. The threats resulting from intentional criminal human activity, which may disrupt the functioning of port facilities, were also presented. The basic and also the most vulnerable facilities of maritime critical infrastructure are seaports. Their safety can be violated from three directions: land, air, and sea. At the same time, it is not possible to ensure the same level of security in all port and land areas. Therefore, port facilities were particularly vulnerable to threats. Ensuring the proper level of port facilities security requires undertaking a number of organizational and technical projects.

Keywords: maritime critical infrastructure, port facility, port security, port security procedures, monitoring systems

Bezpieczeństwo obiektów morskiej infrastruktury krytycznej w aspekcie współczesnych zagrożeń

Streszczenie: W artykule podjęto próbę przedstawienia obiektów infrastruktury morskiej, które mogą lub powinny zostać włączone do obiektów infrastruktury krytycznej. Ze względu na ich charakter i znaczenie dla bezpieczeństwa i gospodarki, obiekty te mogą być klasyfikowane jako krajowe lub europejskie obiekty infrastruktury krytycznej. Przedstawiono również zagrożenia wynikające z umyślnej działalności przestępczej człowieka, która może zakłócić funkcjonowanie obiektów portowych. Podstawowymi i najbardziej wrażliwymi obiektami morskiej infrastruktury krytycznej są porty morskie. Ich bezpieczeństwo może być naruszane z trzech kierunków: lądowego, powietrznego i morskiego. Jednocześnie nie jest możliwe zapewnienie tego samego poziomu bezpieczeństwa we wszystkich obszarach portowych i lądowych. Dlatego też obiekty portowe były szczególnie narażone na zagrożenia. Zapewnienie właściwego poziomu ochrony obiektów portowych wymaga podjęcia szeregu przedsięwzięć organizacyjnych i technicznych.

Słowa kluczowe: morska infrastruktura krytyczna, obiekt portowy, ochrona portu, procedury ochrony portu, systemy monitoringu

Introduction

The concept of critical infrastructure is permanently associated with security and evolves along with civilization changes. The key stage in the protection of critical infrastructure is the correct identification of facilities, equipment, installations, or services whose destruction or disruption of functioning could significantly affect the security of the state and its citizens.

At the same time, a significant part of infrastructure facilities of particular importance for the broadly understood security of the state and ensuring its undisturbed functioning is associated with a special area of the economy, which is a maritime economy. These facilities can be located on sea waters, in the coastal zone, or on the sea coast.

Along with civilization changes, the spectrum of threats to critical infrastructure objects is also changing.

Contemporary challenges in the protection of maritime critical infrastructure go beyond scenarios of interstate conflicts, are more diverse, complex, and unpredictable. The importance of unconventional threats of an intentional nature, asymmetrical threats, which may often be sources of difficulty to identify non-state entities, as well as unresolved regional and local conflicts, and also destabilized countries have increased significantly.

This is due to the fact that more and more often, conflicts are triggered not by states but by various terrorist groups, organized crime, disintegrating national liberation movements, uprisings, and rebellions underlying not only specific political but also religious goals or the usual desire for profit. In such a situation, it is very difficult to solve the problem by precisely determining the opposing party.

Critical infrastructure objects, due to their importance, are subject to special protection which means all activities aimed at ensuring the functionality, business continuity and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities, reduce and neutralize their effects and quickly restore this infrastructure on accident, attacks and other events interfering with its proper functioning (*Act of 22 August 1997*).

As part of the critical infrastructure protection program, the necessary conditions should be created to prevent disruption of critical infrastructure operation, prepare for crisis situations that may adversely affect its functioning, respond to its destruction or disruption, and restore critical infrastructure.

Primarily, owners and operators of critical infrastructure are responsible for ensuring adequate protection, which are the entities responsible for the investment or ongoing operations of its given component, system, or part.

Sea transport accounts for the largest share of overall international trade in goods, and there is a noticeable increase in freight transported by sea regularly. The importance of maritime shipping routes and the scale of trade exchange carried out by sea means that the protection of maritime transport infrastructure has started to be seen as an important dimension of safety. The protection of these facilities is carried out using appropriate organizational measures, supported by technical security systems, such as monitoring systems, early notification, and limiting access to protected facilities and areas.

Identification of Maritime Critical Infrastructure Objects

Critical infrastructure means in Polish legislation: systems and their functionally related objects, including building facilities, devices, installations, services essential for the security of the state and its citizens, and ensuring the smooth functioning of public administration bodies, and also institutions and entrepreneurs *(Act of 22 August 1997)*.

In order to correctly identify critical infrastructure objects in the Government Security Center, two groups of criteria for identifying these objects have been developed. These include system criteria and sectional criteria.

System criteria individually defined for each system characterize quantitatively or subjectively the functions of an object, device, installation, or service, the fulfillment of which may result in being included in the critical infrastructure. On the other hand, the sectional criteria, including victims, financial consequences, the necessity of evacuation, loss of service, reconstruction time, international effect, uniqueness, describe parameters related to the effects of destruction or cessation of an object, device, installation or service.

At the same time, the identification of critical infrastructure objects is carried out in three stages. At the first stage, the selection is made using system criteria. Then, as part of the second stage, using the definition in art. 3 point 2 of the Crisis Management Act, it is checked whether the object, device, installation, or service plays a key role in the security of the state and its citizens and whether it ensures the efficient functioning of public administration bodies, as well as institutions and entrepreneurs. The last, third stage involves assessing the potential effects

of destruction or cessation of potential critical infrastructure. It is implemented using sectional criteria best suited to the characteristics of the given system (*National Critical Infrastructure Protection Program*, 2018, p. 13-14).

According to the Crisis Management Act, critical infrastructure includes systems (*Act of 22 August 1997*):

- energy supply, energy resources, and fuels,
- communication,
- ICT networks,
- financial,
- food supply,
- water supply,
- health protection,
- transportation,
- emergency,
- ensuring continuity of public administration activities,
- production, deposition, storage, and use of chemical and radioactive substances, including pipelines of hazardous substances.

As part of these critical infrastructure systems, it is possible to identify systems, facilities, and services that can be included in maritime critical infrastructure.

Tab. 1. Systems, facilities, and services which may be included in maritime critical infrastructure.

No.	Critical infrastructure systems	Maritime systems, facilities, and services
1.	Energy, energy resources and fuels supply	Power plants using ocean and sea energy to produce electricity Wind farms located in offshore areas Underwater power cables Offshore mining facilities - drilling, production and storage platforms Fuel and energy raw material handling terminals
2.	Communication	Marine communication, navigation, and technical observation systems
3.	ICT networks	Underwater power cables
4.	Water supply	Desalination plants and seawater treatment

No.	Critical infrastructure systems	Maritime systems, facilities, and services
5.	Transportation	Port transshipment terminals Shipping routes Channels
6.	Emergency	Marine rescue
7.	Ensuring continuity of public administration activities	Maritime Offices Harbormasters and harbor officers
8.	Production, stockpiling, storage and use of chemical and radioactive substances, including hazardous substances pipelines	Port chemical transshipment terminals Port warehouses and transmission pipelines Production plants located in ports or their immediate vicinity

Source: own elaboration.

The protection also covers objects particularly important for the security and defense of the state, among which are: objects in which military equipment is produced, renovated and stored [...] seaports of defense significance; [...], facilities directly related to the extraction of: natural gas, crude oil, [...], other facilities being the property of government administration bodies, local government bodies, state institutions as well as entrepreneurs and other organizational units, whose destruction or damage may constitute significant threat to human life and health, national heritage and the environment, or to cause serious material damage and disrupt the functioning of the state (*Regulation of the Council of Ministers of 18 January 2019*).

These facilities include war ports, shipyards in which navy vessels are built and renovated, selected port dangerous goods transshipping terminals, maritime administration facilities, drilling platforms, etc.

Areas, facilities, equipment, and transports important for defense, economic interests of the state, public safety, and other important interests of the state are also subject to mandatory protection by specialized armed protective formations or appropriate technical protection (*Act of 22 August 1997*). Objects classified as maritime infrastructure have also been listed here.

At the same time, recognition of maritime infrastructure facilities in terms of their potential recognition as European critical infrastructure facilities, including:

- sector criteria,
- analysis whether the system or part of the infrastructure is of fundamental importance for maintaining the necessary social functions, health, safety, protection, material, or social well-being of the population, whose disruption or destruction would have a significant impact on the Republic of Poland as a result of the loss of these functions;
- analysis of whether its disruption or destruction would have a significant impact on at least two Member States of the European Union;
- sectional criteria - within the approximate thresholds set by the European Commission and the Member States of the European Union - including the criterion of victims in people, the criterion of economic effects and the criterion of social effects,

certainly allows to include the system of the ocean, short sea, and seaports as European critical infrastructure.

Contemporary Threats for Maritime Critical Infrastructure

Each object, installation, device, or service included in the list of critical infrastructure is potentially exposed to threats that may cause disruption of their work, significant damage, or even their destruction. Such events can often have very severe economic and social consequences.

Threats to port facilities can take the form of internal and external threats. Where a port facility is understood to be a place designated by a Contracting Government or Designated Authority where ship/port relations take place, and port facilities may include areas such as anchorages, sea approaches, and berths for ships (*International Maritime Organization*, 1974).

Internal hazards include fortuitous events, such as environmental pollution caused by the release of toxic substances during transshipment, dust mixtures explosions and fires, technical failures, occurrences resulting from the limited possibilities of handling ships in ports and congestions caused in port facilities, human errors, etc. As external threats to the functioning of seaports, there may be threats resulting from the impact of natural conditions such as storms, icing, precipitation, increased shipping intensity and collision of ships, disruptions in the supply of electricity or from deliberate human activities of a criminal nature,

such as terrorism, cyber terrorism, organized crime or sabotage.

Threats are also armed conflicts, but analysts believe that in the current situation the likelihood of an outbreak of armed conflict of a global and high intensity has significantly decreased, while at the same time, the spectrum of military and non-military activities threatening the security of maritime critical infrastructure, characterized by relatively low intensity has significantly expanded (Mayer, 1992, p. 75).

Therefore, the importance of unconventional intentional threats, i.e., asymmetrical threats caused by non-state actors, terrorists, pirates, or organized criminal groups, has definitely increased.

Contemporary maritime terrorism is understood as a planned and organized attack of violence resulting from political, religious, or ideological motives directed against vessels and carried cargo, port, transshipment, and transmission infrastructure, passengers and crews of ships, navigation infrastructure or offshore hydro-technical constructions. The main goals of modern terrorists at sea can be units transporting energy resources such as tankers, gas carriers, chemical tankers transporting hazardous materials, passenger ships, units in the state service, such as ships, border guard units, ports, port, transshipment and transmission installations, drilling platforms, and other offshore hydro-technical structures, and above all bridges over straits or bays, and navigation markings in narrow and difficult to navigate areas. At the same time, it should be assumed that the most likely locations of the attack facilities will be roads or approaches to ports, port facilities and terminals, narrow areas and approaches to these areas, global or regional shipping hubs and areas of exploitation of marine oil and natural gas resources.

It should be noted that the potential targets of the attack in the case of the coast and coastal agglomerations are primarily: seaports, shipyards, state and local government administration facilities, places of significant clusters of people and industrial facilities, etc. (Kubiak, Makowski, Mickiewicz, 2005, p. 73).

Identifying real threats is a key process in managing critical infrastructure security. The results of this process are used when developing critical infrastructure protection plans containing their detailed characteristics and risk assessment of their occurrence and event scenarios.

In the case of seaports, the targets of such attacks may be the port facilities themselves as well as ships mooring in ports or standing on roads or adjacent waters.

The attractiveness of seaports as the goals of potential asymmetrical activities is due to:

- the importance of ports for the macroeconomic system of the national economy,
- collection on a relatively small area of fixed assets of considerable value,
- the presence within the ports of ships of various flags, including countries that are parties to the international crisis or are in conflict with terrorist organizations,
- large port areas of land and water, which hinders the organization of an anti-infiltration system,
- location of ports in the vicinity of large agglomerations,
- the possibility of influencing the operation of ports through activities within generally accessible maritime areas,
- limited possibility of counteracting terrorist actions without disorganizing the work of ports.

The analysis of previous activities allows to assume that attacks on port facilities and ships moored in the port may take the form of bombings, short-term fire impact on a selected object, control by a terrorist group of a port facility or a ship moored in the port (infiltration onboard), deliberate technical failure within the port infrastructure, attacks using NRBC (nuclear/radiation, biological and chemical) and cyber-attacks (Bursztyński, 2011).

Considering the security of the port as a point element of the transport system, located at the interface between the land and the sea, where due to the technological barrier there is a change in the means of transport from land to sea or vice versa, one should take into account the possibility of threats from three directions: land, sea, and air. When considering hazards from the sea, both hazards from the sea surface and the sea depth should be taken into account.

Landside attacks can be carried out in the form of bomb attacks using vehicles filled with explosives (cars, trucks, cisterns), entering port facilities, or parked in their vicinity. Explosives may also be delivered to port areas in the form of postal items, with supplies for units mooring in the port or even by trained dogs. Also, people threatening the security of the facility may enter the port areas from the land side, in order to disrupt its operation or to sabotage it.

Attacks from the sea can be carried out using surface and underwater units. The means of transport that could be used by potential terrorists include such as surface or underwater vessels: boats, fast motorboats, water scooters, ships with dangerous cargo such as tankers or even passenger vessels, and miniature

submarines. Small vehicles transporting scuba divers and swimmers DDV/SDV (Diver Delivery Vehicle/Swimmer Delivery Vehicle), vehicles UUV (Unmanned Underwater Vehicle) and even individual divers can also be used to carry out an attack on the port facility from the seaside, scuba divers or swimmers on the surface of the sea. The activities of scuba divers and other underwater diversion forces and means may be primarily focused on placing explosives in the underwater parts of the hulls of vessels standing in the port or under important port infrastructure devices.

Another form of threat to port facilities or mooring units in the port is the short–term fire impact that can be carried out using hand–held machine guns, grenade launchers, mortars, recoilless cannons, and guided or unguided lightweight missiles. Potential platforms for moving these weapon systems can be land–based motor vehicles or seaside vessels such as manned and unmanned high–speed surface motorboats. The use of improvised explosive devices (IEDs), which are increasingly used by terrorists outside the area of military operations, and have become the most dangerous weapon in their hands over the past decade, cannot be ruled out (Cywiński, 2017, p. 309).

Aerial attacks can be carried out using manned and unmanned aerial vehicles as well as remotely controlled flying models, drones, and even balloons.

Cyber-attacks on port information systems can take the form of spam that interferes with the operation of information exchange systems, compromised classified networks, send false alarm messages, trigger alarm systems, steal personal data, falsify and block information, change databases, etc..

Other forms of attacks on port facilities can be various methods of interfering with the proper functioning of these facilities, such as demonstrations, blockades, or riots in ports or their direct surroundings.

It can also be assumed that during asymmetrical attacks on seaports, individual forms of impact and carriers of threat will be used alone or in combination, and the main goal will be to make the greatest possible damage and cause significant losses and disorganize the functioning of the attacked port and cause an emergency.

Security Organization of Port Facility

Contemporary intent threats have forced the implementation of appropriate procedures and security measures not only on vessels but also in the areas of seaports as land-sea contact areas where cooperation between the ship and the

port facility is achieved. Due to the size of port areas, their diversity resulting from their function and their land and water nature, as well as the fact that they are to a large extent public areas or directly border such areas, it is impossible to ensure an equal level of protection throughout the entire port. In relation to the above, port facilities and areas were designated, referred to as port facilities, constituting separate parts of the port, which are autonomous areas in terms of security.

Ensuring the safety of port facilities is a multidimensional chain of consolidated activities, including preventive measures, procedures performed during daily operation, practical checking in the operation of emergency procedures, and in the event of a real threat, also taking appropriate actions and eliminating the effects of the threat.

In order to ensure proper protection of port facilities, systemic solutions have been adopted, among which the requirements of the ISPS Code have become a fundamental tool. This code obliged maritime administration authorities, shipowners, and entities managing port facilities to implement the indicated procedures and security measures at subordinate facilities and to ensure the exchange of information and coordination of actions in the event of threats.

Pursuant to the provisions of this document, a port facility security assessment must be carried out for each port facility, and a port facility security plan must be developed based on that. A port facility security officer is also appointed to maintain the security system for a given port facility.

The main purpose of the ISPS Code is to provide a framework for cooperation between Contracting Governments, local maritime administration, and shipping companies. This is due to the fact that the Code includes general guidelines that every facility manager must adapt to the needs of a given port facility in order to implement an appropriate security system. To achieve the objectives of port facility security, the Code sets out the necessary functional requirements.

In accordance with these requirements are as follows:

- collecting and assessing information on threats to port facilities and exchanging this information between contracting governments in this regard;
- prevention of unauthorized access to maritime units, port facilities or their prohibited zones and introduction of procedures and precautionary measures by developing a security assessment and security plan for each ship and port facility;
- introduction of procedures for the control of persons and cargo to prevent the transfer of illegal weapons, flammable and explosive materials to port facilities

and on ships' boards;
- providing means to enable the alert to be taken to counter threats or security incidents;
- enabling and implementing systems and procedures for effective communication between a maritime unit and a land base;
- conducting training, trial alerts, and practical exercises at specified intervals to become familiar with the requirements of security plans and procedures regarding the principles of behavior in an emergency, the use of security measures, and the exchange of information;
- appointing functional persons responsible for the implementation and execution of the provisions of the Code.

In order to properly implement the tasks arising from the Code, manager for each port facility is appointed by the port facility - Port Facility Security Officer – PFSO (in Polish: Oficer Ochrony Obiektu Portowego – OOOA), for each ship the managing body - the shipowner shall appoint the Company Security Officer – CSO (in Polish: Oficer Ochrony Armatora) and also Ship Security Officer – SSO (in Polish: Oficer Ochrony Statku) (International Ship Suppliers & Services Association, 2016, p. 2).

Technical Systems Supporting Port Facility Protection

The port area should be secured from the land and seaside with specially adapted equipment for this purpose; all employees and other persons staying in the port area should be carefully checked. National legislative documents set out rules for the protection of shipping and seaports, including the protection of life and health of persons in seaports, port facilities, or ships (*Act of 29 October 2010*).

In the Regulation of the Council of Ministers of 15 April 2011 on control methods and measures in the field of shipping and maritime security, technical security measures have been presented for a port, port facility, and ship security (*Regulation of the Council of Ministers of 15 April 2011, §3.1*). Among these measures were alarm and monitoring systems and devices, wired or wireless communication between guard posts and duty services, fences securing access from land and sea, the lighting of facilities and warning boards.

The main tasks of security systems include security measures (protection) against causing crisis situations in facilities and systems referred to as critical infrastructure, i.e., counteracting causing a threat, or disrupting the functioning of the facility.

The port security system should consist of components which include: shoreline surveillance system, land and water protection, protection of critical facilities for port operation, monitoring of vessel movement, and response force.

The seaport area is usually divided into two parts: the open (for general use) part with the system, and the closed part protected by specialized security services, and access to the closed part from the land side is limited by the use of fences, passes control, active patrol and technical protection systems. The port security system should include permanent 24–hour outlets at port gates, 24–hour motorized patrols, porters in selected port facilities, service for alarm monitoring and video monitoring stations, electronic protection of selected objects and rooms, passenger, car, and material pass systems and occasionally issued in connection with the arrival of passenger ships or the introduction of a higher level of protection sentry posts and pedestrian patrols.

Systems of technical protection of port areas include protection of the external areas and mechanical security, access control, burglary and assault signaling, utility television, radio-electronic protection, alarm systems, and transmission as well as alarm monitoring, fire signaling, monitoring of environmental, industrial and technical hazards.

Area protection systems are used to protect large, open spaces in seaports, which record the crossing of physical or electronic barriers. These systems can use both spatial sensors and video sensors.

Access control is the most common method of ensuring the safety of facilities and vessels moored in ports from the land side. The port facilities use electronic identification and access control systems equipped with numeric code readers, electronic identification cards, biometric features, or optical document readers.

Entries and exits of motor vehicles, including trucks, should take place, after prior inspection, through gates that are locked every time they are not used. Drivers, helpers, and passengers should also be carefully monitored.

Systems for technical observation of the surface and the underwater situation around the port should make it possible to detect the threat necessary in advance, enabling the necessary security measures to be taken. For this reason, they should cover the range of maritime areas of the port and the approach fairways, diversified in terms of distance and depth.

The systems cooperating with radars allow for automatic identification of vessels as well as the recording of images from monitors and also conversations

with vessels' crews. These systems were used to control ship traffic in areas characterized by high traffic volumes, a large number of vessels in narrow passages, or navigational hazards (Vessel Traffic Service systems - VTS).

In order to monitor the situation on the sea surface, optoelectronic video monitoring systems are also used, including observation, detection (motion detection), intelligence (analysis of changes in the scenery of the environment), and network (using the Internet Protocol). To monitor the sea level, acoustic and non-acoustic devices are used to observe zones varying in distance and depth. The hydroacoustic devices used in port security systems include passive acoustic antennas, medium-range active sonars, and high-range short-range active sonars. Acoustic systems using different types of sonars are very often supplemented with other solutions, which include active acoustic barriers as well as measuring buoys or hydro-buoys. Depending on the configuration, the barriers may consist of a system of several or several hydroacoustic transceivers, supplemented with data processing and acquisition systems. Measurement buoys can be independent measurement systems anchored near the port approach (Pozański, 2011, p. 22-24) Non-acoustic systems include systems using magnetic field sensors, electric field sensors, and underwater electro-optical monitoring systems.

Highly sensitive magnetic transducer systems detecting local magnetic anomalies caused by objects moving in the sea are used for continuous and automatic monitoring of the underwater situation in the areas of sea bases and ports. The shortest range among underwater situation monitoring systems is characterized by underwater optoelectronic systems providing high-resolution color images.

Physical barriers constitute the last zone of protection for ports and berths of ships. The main purpose of their use is to prevent unauthorized, physical intrusions into a secured water area or terrorist suicide attacks using fast motorboats on vessels mooring in ports or on important port facilities. Barriers can also be treated as the boundaries of safety zones designated in port areas or areas closed for navigation.

Physical barriers can occur in two variants: as fixed barriers (Fixe Security Barriers - FSB) and floating barriers (Port Security Barriers - PSB). Physical barriers occur in the form of fixed or floating nets, floating booms, and partitions, or even barges anchored in port basins.

Summary

Seaports are extremely important for the economy facilities, classified as critical infrastructure, and due to their international significance also as European critical infrastructure. In the current situation, seaports are more exposed to asymmetrical activities than to attacks during open armed conflict. Therefore, the priority task is to secure these objects against intentional unlawful actions aimed at disrupting their proper functioning.

Potential terrorists are unlikely to be able to carry out large-scale operations when attacking ports and the vessels mooring in them or ships anchored inroads. However, taking into account the importance of maritime transport for the global economy, it should be assumed that even single attacks can cause significant damage and losses, and a wide spectrum of threats necessitates the need to protect ports and port facilities both from the sea and land.

The entry into force of the provisions of the ISPS Code has become a tool enabling the introduction of measures to improve marine security. It also imposed new tasks and responsibilities on shipowners, state administrations, port facility managers as well as ship crews.

However, the security systems implemented at port facilities are mainly preventive, and their main task is to prevent security incidents. The overall integrated actions are therefore designed to prevent the emergence of a threat, and in the event of its occurrence take immediate protective action.

In order to detect threats early and enable the necessary preventive measures to be taken, technical systems are used to monitor port areas to detect and identify potential threats early. Integrated port security systems use devices that monitor and identify the surface and underwater situation, enabling the detection and tracking of objects violating the protected area. In this case, monitoring means regular qualitative and quantitative measurements of specific phenomena or detection of the presence of specific objects, carried out for a specified period of time in the waters around the port and in the areas of the port itself. These systems include long-range radars and coastal passive and active sonars, magnetic barriers, acoustic and chemical detectors, optoelectronic sensors, visual observation systems, and fixed and floating physical protective barriers. The devices operating within these systems cover zones varying in distance and depth from the protected object. At the same time, the distance of detection and identification of the threat

should enable the development of the decision to issue an alarm and the effective avoidance or repression of the attack, using the appropriate response method for the given system.

Due to constant changes in the surrounding environment, including changes in methods and techniques used by modern terrorists, protection procedures and supporting technical systems are also constantly changing and modernizing.

References

Amendments to the International Convention for the Safety of Life at Sea, 1974, adopted by the International Maritime Organization on December 13, 2002 (Journal of Laws of 2005, No. 120, Item 1016).

Bursztyński, A. (2011). Organizational measures to ensure the safety of stopping vessels in ports and naval bases of the Polish Navy. *Scientific Journal of Polish Naval Academy*, *52*(186A), 13-30. Accessed: http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-2843b7d8-6db3-4997-aa88-c8d112ef1f68 [30.03.2020].

Cywiński, A. (2017). The IED – the Present Danger for Critical Infrastructure and State Security. *National Security Studies*, *7*(12), 305–333. Accessed: https://studiabn.pl/resources/html/article/details?id=179646 [15.04.2020].

International Ship Suppliers & Services Association (2016). *International Ship and Port Facility Security Code. ISPS Code Guidelines for Ship Suppliers.* London: International Ship Suppliers & Services Association. Accessed: https://shipsupply.org/wp-content/uploads/2017/01/ISPS-Code-ISSA-Guidelines-Aug-2016.pdf [10.04.2020].

Kubiak, K., Makowski, A., Mickiewicz, P. (2005). *Poland and threats of maritime terrorism.* Warszawa: Publishing House TRIO.

Mayer, V. A. (1992). Naval Surface Warfighting Vision 2030. *Naval Engineers Journal, 104*(3), 74–88. DOI: https://doi.org/10.1111/j.1559-3584.1992.tb02226.x.

National Critical Infrastructure Protection Program (2018). *Resolution No. 121/2018 of the Council of Ministers of September 7, 2018 amending the resolution on the adoption of the National Critical Infrastructure Protection Program*. Accessed: https://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf [10.04.2020].

Pozański, P. (2011). Contemporary threats to the elements of maritime infrastructure and their detection systems. *Polish Hyperbaric Research*, *35*(2), 7–34. Accessed: http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BAT1-0039-0005 [10.04.2020].

Regulation of the Council of Ministers of 15 April 2011 on control methods and measures in the field of shipping and maritime security (Journal of Laws of 2011, No. 93, Item 539 as amended).

Regulation of the Council of Ministers of 16 December 2016 amending the regulation on objects of particular importance for the security and defense of the state and their special protection (Journal of Laws of 2017, Item 42).

Regulation of the Council of Ministers of 18 January 2019 amending the regulation on objects of particular importance for the security and defense of the state and their special protection (Journal of Laws of 1997, Item 250).

The Act of 22 August 1997 on the protection of persons and property (Journal of Laws of 1997, No. 114, Item 740 as amended).

The Act of 26 April 2007 on crisis management (Journal of Laws of 2007, No. 89, Item 590 as amended).

The Act of 29 October 2010 amending the act on crisis management (Journal Of Laws of 2010, No. 240, Item 1600).

The Act of 4 September 2008 on the protection of shipping and seaports, (Journal of Laws of 2008, No. 171, Item 1055 as amended).