Daria Olender, PhD
Department of Economic Law and Commercial Law
University of Warmia and Mazury in Olsztyn
Centre for Baltic Sea Region Security
ORCID: 0000-0002-5786-8113
e-mail: daria.olender@gmail.com

# UNMANNED SURFACE AND UNDERWATER PLATFORMS AS A NEW CHALLENGE AND THREAT TO CRITICAL MARITIME AND PORT INFRASTRUCTURE

**Summary**

There is growing concern about the threat that unmanned platforms pose to state security. Ensuring protection against such threats is a growing scope in planning for the protection of critical infrastructure facilities. This is important because, at the moment, there are no standards in terms of security, including information security, for any infrastructure that is not on land. Due to volume limitations arising from the very nature of the publication, the author focused on selected aspects of the presented issue. However, achieving this goal required finding answers to three intermediate questions regarding the challenges of operating maritime infrastructure, defining threats from surface and underwater drones, and identifying measures aimed at ensuring protection in the subject area.

**Keywords:** safety, security, unmanned platforms, surface and underwater platforms, drones, sabotage, critical infrastructure.

## INTRODUCTION

There has recently been a growing concern about the threat posed by unmanned platforms to national security. Ensuring protection against such threats constitutes an ever-growing scope (aspect, area, occupies more and more space) in planning for the protection of critical infrastructure facilities. To date, little attention has been paid to threats to maritime and port infrastructure in the Polish discourse[1], even though this type of infrastructure has been significantly developed in Poland in recent years, for

[1] R. Miętkiewicz, Wykorzystanie bezzałogowych jednostek nawodnych w zabezpieczeniu morskich obiektów infrastruktury krytycznej, Akademia Marynarki Wojennej, Gdynia 2018; Idem, Systemy autonomiczne w działaniach na morzu, Akademia Marynarki Wojennej, Gdynia 2023; M. Piekarski, Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych, Ekspertyzy PTBN 2023, No. 1; K. Gawrysiak, Zagrożenie infrastruktury krytycznej polskich portów morskich pochodzące z kierunku podwodnego, ”Gospodarka Materiałowa i Logistyka” 2017, No. 12, p. 228-252; A. Bursztyński. Bezpieczeństwo obiektów morskiej infrastruktury krytycznej w aspekcie współczesnych zagrożeń, ”Rocznik Bezpieczeństwa Międzynarodowego” 2020, No. 14(1), 167–182.

instance, completed investments such as the LNG terminal[2] and the incomplete Baltic Pipe natural gas pipeline[3] (FSRU terminal[4]). Accordingly, many of them are located on the Polish coast and in the Polish zone of responsibility in the Baltic Sea.[5] Since the vast majority of these investments are part of the strategy to diversify the supply of raw materials, they serve to guarantee energy security for the Republic of Poland. The construction of the OWF is still being planned.[6] The war in Ukraine has already highlighted the importance of keeping maritime infrastructure secure. For example, port blockades have prevented the transport of foodstuffs. Attacks involving platforms (flying, surface or underwater) pose a major threat to maritime facilities, not just vessels, but especially port facilities or other infrastructure, such as the Crimean Bridge. However, kinetic operations are not the only threats.

Following the Russian Federation's aggression against Ukraine and the repercussions resulting from international sanctions, the role of Poland as a player in the energy supply market is increasing. Poland, being a frontline state and one of the biggest opponents of the Russian invasion of Ukraine, has to recognise that the Kremlin will carry out actions aimed at undermining Poland's image in the international arena, resorting to actions of a hybrid nature, among others.

The possibility of the hostile use of unmanned water platforms (both surface and underwater) has not been studied in detail so far. The author

[2] LNG terminal is ”a specialised port designed to handle ships carrying liquefied gas. Usually there are storage tanks for the transshipped gas on the premises of the gas port”. In: D. Konkol, T. Perka, Polskie porty morskie, Dom Wydawniczy Księży Młyn, Łódź 2011, p. 123.
Poland's first offshore transhipment and regasification terminal for liquefied natural gas (LNG), was built as an alternative to the direction of supply from the gas tycoon, i.e. the Russian Federation; it makes it possible to receive ‘blue fuel’ from other directions, via the sea route, which serves to increase the level of energy security (also economic) of the Republic of Poland. It is the only facility of this size in Central and Eastern Europe and one of the largest on the Old Continent.
See more in: W. Jędrzejewski, Terminal LNG w Świnoujściu a integracja środkowoeuropejskiego rynku gazu (in:) Piątek J.J., Podgórzańska R. (ed.): Terminal LNG w Świnoujściu a bezpieczeństwo energetyczne regionu i Polski, Wyd. Adam Marszałek, Toruń 2013, p. 27-28; W. Jakóbik, Opracowanie: Gazoport w Świnoujściu wpłynie na rynek w Europie, projekt w Kłajpedzie jest kluczowy głównie dla Litwy, http://jagiellonski.pl/?p=3022 (21.09.2014); Olender D., Działania Policji w zakresie ochrony przed terroryzmem nowo powstającego terminalu LNG w Świnoujściu [in:] Bezpieczeństwo. Zagadnienia, K. Kraj (scientific ed.), WSIiZ, Rzeszów 2013, p. 79-80; Olender D., Gazoport w Świnoujściu jako potencjalny cel terrorystów, Zeszyty Doktoranckie Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej” 2013, No. 3(8), Warsaw 2013, p. 74; World’s LNG Liquefaction Plants and Regasification Terminals, accessed on http://globallnginfo.com/GLNG_Database.aspx (01.05.2024);

[3] The so-called Baltic Corridor, Baltic Gas Pipeline. A strategic infrastructure project focusing on the construction of a new gas supply corridor for the European market, resulting in the launch of a gas pipeline system connecting Norway, Denmark and Poland with a capacity of 10 bln $m^3$ per year on 27 September 2022.
It must be stressed that the Baltic Pipe constitutes a link in a broader project referred to as the so-called Northern Gateway, which aims to increase the security and diversification of the supply of ‘blue fuel’ and to create competitive gas markets in the Central European and Baltic regions (through the Baltic Gas Pipeline and the Świnoujście Gas Port).

[4] Floating terminal in the Gulf of Gdansk.

[5] Which, of course, does not mean that these investments are limited to this area.

[6] Offshore wind energy appears to be one of the most rapidly growing renewable energy sectors in Europe. According to projections, the first offshore wind farms, sited in the Polish Exclusive Economic Zone in the Baltic Sea, will start producing energy in 2026. See more in: Program rozwoju Morskich Farm Wiatrowych, accessed online: https://www.gov.pl/web/morska-energetyka-wiatrowa/program-rozwoju-morskich-farm-wiatrowych (31.05.2024).

intends to fill the gap identified in this area and present possible consequences of the use of unmanned platforms on maritime and port infrastructure, thus filling the research gap to some extent. Given the limitations in terms of volume due to the nature of this paper, the author focuses on selected aspects of the issue being discussed. However, achieving this objective necessitated finding answers to three intermediate questions regarding challenges to the functioning of maritime infrastructure, defining threats posed by surface and underwater drones and indicating actions aimed at ensuring protection in the field in question.

## EUROPEAN AND NATIONAL CRITICAL INFRASTRUCTURE AND ITS MARITIME DIMENSION

When writing about critical infrastructure (CI) in the context of the maritime area of the Republic of Poland, it is impossible not to mention European Critical Infrastructure. This issue was introduced into the Polish legal system by the Act of 26 April 2007 on crisis management as a result of the implementation of the provisions of the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures.[7] According to the aforementioned EU document, critical infrastructure means "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[8] In turn, European Critical Infrastructure (ECI) means "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure."[9] ECI comprises systems and functionally related facilities, equipment and installations crucial to the safety of the state and of its citizens. They play a role in ensuring the smooth functioning of public administration bodies, institutions, and businesses. These are designated in systems that supply energy, raw materials, fuels and transport systems to supply electricity, oil and natural gas, rail, air transport, inland waterways, ocean shipping, short sea shipping and ports.[10]

Critical infrastructure includes "systems and their functionally related facilities, including buildings, equipment, installations, services that are crucial to the security of the state and its citizens and that serve to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs."[11]

[7] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345/75 of 23 December 2008).
[8] Directive on the Identification and Designation of European Critical Infrastructures…, Article 2(a).
[9] Ibidem.
[10] Act on crisis management…, Article 3(2a).
[11] Ibidem, Article 3(2) indicates that critical infrastructure includes: " systems for the supply of: energy, energy raw materials and fuels; communications; ICT networks; financial; food supply; water supply; health care;

The protection of CI and ECI is identical in nature – it involves ”all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructure with a view to preventing, mitigating and neutralising threats, risks or vulnerabilities, and recovering them rapidly in the event of failure, attack or other disruptive event.”[12]

The wording of the definition of CI makes it possible to consider that, concerning maritime and port infrastructure, its designatory scope extends to systems and their constituent functionally related facilities.[13] The same is true for the European dimension of the infrastructure in question.

Such a view of critical infrastructure is presented in the literature. D. Dmowski points out that ‘in the maritime context, critical infrastructure includes strategic assets such as ports, shipyards, energy, oil and gas installations, as well as navigation and communication systems. Each of these elements is crucial to defence operations, logistics and support of military and civilian activities at sea”.[14] Sea ports, in particular, are “considered key points in logistics chains, essential for military transport, supply and support of naval operations.”[15]

Concerning the facilities, installations, equipment, and services that make up critical infrastructure, particularly regarding the maritime aspect, there is little information available because the list is classified. Based on the detailed criteria referred to in paragraph 2(3), the Director of the Governmental Security Centre, in cooperation with the relevant ministries responsible for the systems, draws up a list of facilities, installations, equipment and services constituting critical infrastructure, all broken down by individual systems.[16] It should be noted that this list also distinguishes between European Critical Infrastructures located in the territory of the Republic of Poland and European Critical Infrastructures located in the territory of other Member States of the European Union that are likely to have a significant impact on the Republic of Poland.[17]

It is important to note that there are currently four key seaports in Poland, located along its coastline. These are Szczecin and Świnoujście in Western Pomerania, as well as Gdynia and Gdańsk in the Gulf of Gdańsk. These ports handle goods of strategic importance.[18] The Act on Sea Ports and Harbours defines them explicitly as ”ports of fundamental importance for the national economy.”[19] A gas port is located in the west, and an oil port is located in the Gulf of Gdansk. Whether they are ports, terminals (gas, oil, or transshipment), energy installations, bridges, submarine cables or other

transport; rescue; ensuring continuity of public administration; production, storage, warehousing and use of chemicals and radioactive substances, including pipelines for hazardous substances”.

[12] Ibidem, Article 3, item 3.

[13] Following the provisions of the Act on crisis management in Article 3, item 2.

[14] R. Dmochowski, Strategiczne fundamenty bezpieczeństwa morskiego (analiza), https://portalstoczniowy.pl/strategia-fundamenty-bezpieczenstwo-morskie-ochrona-infrastruktura-krytyczna-globalny-system/ [accessed on: 01.06.2024].

[15] Ibidem.

[16] Act on crisis management…, op. cit.., Article 5b, par. 7, item 1.

[17] Ibidem.

[18] Including military cargo. Furthermore, Gdynia and Świnoujście are ports which are permanent sea bases used by the Polish Navy.

[19] Act on Sea Ports and Harbours…, Article 2, item 3.

facilities, they require enhanced protection against actual and potential threats.

## CHALLENGES AND THREATS TO THE SECURITY OF PORT AND MARITIME CI

What makes Poland stand out in Europe is unquestionably its geostrategic location. This position requires increased multifaceted protection of individual sections of the border. The length of the maritime border reaches 500.94 km.[20]

Implementing innovative projects in order to become less dependent on energy resources from the east is going to play a significant role in the near future. Solutions in the form of offshore wind energy (OWE) require support in the form of installation and service ports. In addition, the construction of a nuclear power plant also requires consideration of the safety of facilities and installations, drawing on the experience of other states.

However, one should be aware of the need to protect critical infrastructure facilities (primarily systems for energy supply, raw materials and fuels, ICT networks, transport and production, storage, warehousing and use of chemical and radioactive substances). Ensuring the continuity of the functioning of infrastructure, i.e., the continuity of uninterrupted supply, is a priority in this respect. The problem of restoring CI also remains a major challenge. This issue escalates into a problem if we look at the location - a harsh, unforgiving marine environment.

Threats (regardless of their degree and nature) can lead to significant changes in the functioning of facilities and consequently affect the level of security of the state and its citizens. One of the most serious threats in this regard appears to be of a terrorist, sabotage or diversionary character. This is where modern technologies such as unmanned units come into play.

## SURFACE AND UNDERWATER DRONES

[20] Granice RP, accessed online: https://www.strazgraniczna.pl/pl/granica/granice-rp/1910,Granice-RP.html (21.05.2024).
It should be noted that there are several of these borders: the coastline, which – excluding the internal waters of the Szczecin Lagoon and the Vistula Lagoon – is 524 km (together with the coastline of the above-mentioned gulfs, it covers a total of 770 km); the territorial sea boundary – 440 km; the exclusive economic zone (EEZ) boundary – the external boundary of this zone, i.e. from the side of the open sea, is 557 km (after an almost 40-year dispute over the course of the boundary between the exclusive economic zones of Poland and Denmark, the boundaries of the Polish EEZ were changed - the long-standing dispute covered 3540 km$^2$ of the Baltic Sea area. On 19 November 2018, an agreement on the demarcation of maritime areas and, in effect, on the division of the disputed area was signed (it entered into force on 28 June 2019). As a result of the agreement, 2834 km$^2$, i.e., 80.1% of the disputed area, went to Denmark, while 706 km$^2$, i.e., 19.9% of the area, went to Poland. Currently, the total area of the Polish EEZ is 19730 km$^2$. See more in: Maritime boundaries between Denmark and Poland, IILSS – International Institute for Law of the Sea Studies, accessed online: http://iilss.net/maritime-boundaries-between-denmark-and-poland/ (21.05.2024); Over 40 years of conflict is over: Denmark & Poland agree on border, accessed online: https://energywatch.com/EnergyNews/Policy___Trading/article10981245.ece (21.05.2024); Poland and Denmark sign agreement on maritime boundary in the Baltic Sea, accessed online: https://maritime-spatial-planning.ec.europa.eu/events/poland-and-denmark-sign-agreement-maritime-boundary-baltic-sea (21.05.2024).

"Drone operations were not really possible on a larger scale up until today, but currently (...) the technology is available at a relatively low cost".[21]

"UAVs enable the delivery of different types of intelligence or perform specific actions. They replace humans in demanding situations and locations, bringing benefits in terms of cost, time and safety".[22]

Automated vehicles are an effective solution for exploring hard-to-reach environments. It is important to recognize that at sea and underwater, visibility is often lacking. In maritime settings, drones present significant advantages, including their small size and low operating costs. Additionally, they may also be capable of conducting attacks.[23]

## Surface and underwater drones – a modern challenge and a threat

The offensive potential of drones can pose a threat to vessels, submarines, oil platforms, port installations and submarine cables. It is not impossible or particularly challenging to equip them with explosives.[24] It is important to note that they are essential for developing anti-drone measures.

One specific threat is that they can be used to sabotage the operation of communication networks or navigation systems, creating a real risk of collision or accident with other vessels. This, in turn, poses a threat to safe navigation. This does not have to have a spectacular outcome in the form of a direct attack on vessels. Instead, what counts is the effect of demonstrating the weakness of the state authorities - a distorted image of the state in front of the public, who will feel 'unprotected', or in a weakened image in the international arena.

Another threat is the use of drones for intelligence gathering, e.g., in the form of mapping secret sea routes, revealing specific coordinates of hazardous material storage sites (including the location of chemical weapons and ammunition dumped in the Baltic Sea[25]) or monitoring activity in ports (especially currently, when arms shipments for Ukraine are being unloaded in a Polish port).[26] Gathering intelligence can be used in the future by the

[21] M.J. Dougherty, Drony. Ilustrowany przewodnik po bezzałogowych pojazdach powietrznych i podwodnych, Wyd. Bellona, Warsaw 2015, p. 216.

[22] W. Wyszywacz, Drony, Wyd. II rozszerzone, Wyd. Poligraf, Brzezia Łąka 2020, p. 27.

[23] See more in: M.J. Dougherty, Drony. Ilustrowany przewodnik…, op. cit., p. 60-61.

[24] "On 21 September, two surface drones of unknown type were observed near the Russian WMF Black Sea Fleet base in Sevastopol on the Black Sea. (…) The unmanned aircraft was equipped with a jet propulsion system and designed to operate in shallow waters. Its shape was designed to make it difficult to detect by radar systems. (…)". The second "unmanned vehicle was equipped with numerous sensors. A camera and an infrared functioning device were mounted on its low mast. (…) Two sensors were also mounted in the bow section. These are probably remote detonators. This is because the UAV was filled with explosives and was used to attack surface vessels." As cited in: T. Hypki, Wojny bezzałogowców, "Raport. Wojsko, technika, obronność" 2022, No. 11, p. 5. …

[25] See more in: J. Michalak, Bezpieczeństwo morskie państwa wobec zagrożeń generowanych przez zatopioną amunicję chemiczną, AMW, Gdynia 2018, p. 91-110.

[26] This only strengthens the intelligence capabilities of foreign agencies. China's Hutchinson Port Holdings leases a section of the quay (container terminal in Gdynia), located a few hundred metres away from the dock where the unloading of arms supplies to Ukraine takes place. The past of the owner, a Chinese tycoon, is no secret, and it is even more worrying that it is allowed to operate in such close proximity to a Polish military port.

agents of foreign countries to carry out diversionary activities, sabotage or acts of a terrorist nature.

Drones can operate in a very unobtrusive manner, which means they are very difficult to detect. Underwater drones are able to operate at considerable depths, away from radar and monitoring systems. Surface drones, on the other hand – can be small and inconspicuous, which in turn makes them difficult to identify. Remote exploitation of the seabed is now possible, highlighting the urgent need to protect undersea cables, as their current status is unsatisfactory. 'Underwater communication cables, frequently referred to as <<the nerves of the digital world>>, are key elements of the telecommunications infrastructure, essential for the circulation of data and information on a global scale. From the military point of view, these <<information highways>> represent both a strategic resource and a potentially critical point in the national security context of any country with access to the sea."[27]

The maritime environment can also provide a desirable setting for terrorist activities, especially if the target facility has a leading role in security in a wider context. A high-profile terrorist attack targeting a vital link in a state's security infrastructure would be considered a huge success in the list of global terrorist achievements, as the phenomenon of terrorism is associated with a desire to attract public and mass media attention, instigate fear and insecurity and highlight vulnerabilities of state authorities.[28]

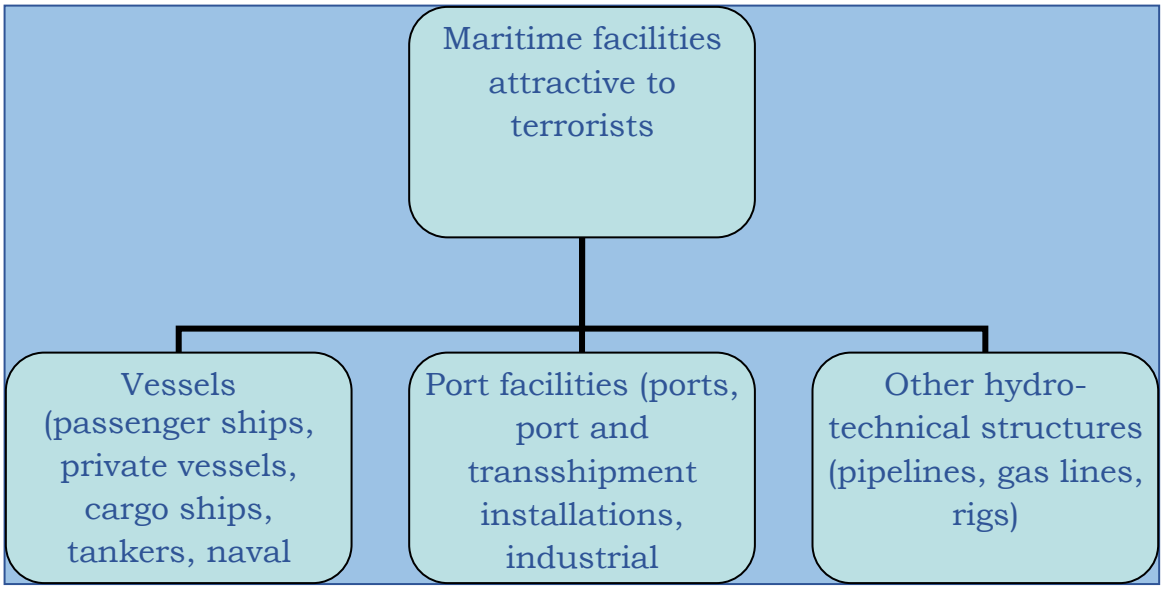
The analysis of past attacks, the nature of maritime transport and the peculiarities of maritime hydro-technical structures allow the identification of potential objects of maritime terrorism (Figure 1).[29]

Figure 1: Potential targets of maritime terrorism

[27] R. Dmochowski, Strategiczne fundamenty bezpieczeństwa morskiego…

[28] D. Olender, Gazoport w Świnoujściu jako potencjalny cel terrorystów, "Zeszyty Doktoranckie Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej" 2013, No. 3(8). Warsaw 2013, p. 79.

[29] In the 1960s, a form of maritime violence emerged that could not be categorised as "maritime piracy" nor "maritime guerrilla warfare" – maritime terrorism. The era of maritime terrorism opened with the 1961 hijacking of the passenger liner Santa Maria. This was followed by a succession of ideologically and politically motivated attacks targeting not only passenger vessels, but e.g. oil tankers, destroyers, as well as ports and port or transhipment installations.




Source: Own elaboration based on T. Szubrycht, Morskie aspekty międzynarodowego terroryzmu
(in:)
M. J. Malinowski, R. Ożarowski, W. Grabowski (ed.): Ewolucja terroryzmu na przełomie XX i XXI wieku, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2009, p. 167.

The above described is a global take, until recently the most commonly cited.

The gradual increase in the circulation of hazardous cargo (oil and its derivatives, gases, chemicals, nuclear waste, explosives, etc.) makes the risk of an unexpected terrorist attack seem increasingly real. Experts point out that the sites of potential attacks include port facilities or terminals, roadsteads or port entrances, global or regional shipping hubs, and areas of intensive exploitation of offshore oil and gas resources.[30]

However, due to the limitation of volume due to the nature of this paper, the focus should be on the Polish domestic situation and potential threats to fixed infrastructure and services.

In view of the above, professional protection of LNG terminals is of vital importance. As a seaport, the LNG terminal in Świnoujście, due to its location, requires protection against terrorist threats from land, air and sea.[31]

There has been a rapid development of unmanned platform technologies – both aerial and marine (surface and underwater) in recent years.[32] Globally – on 29 July 2021, they were used in a new form of terrorist

[30] T. Szubrycht, Morskie aspekty międzynarodowego terroryzmu (in:) M. J. Malinowski, R. Ożarowski, W. Grabowski (ed.): Ewolucja terroryzmu na przełomie XX i XXI wieku, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2009, p. 167.

[31] K. Kubiak, Przemoc na oceanach. Współczesne piractwo i terroryzm morski, Wyd. TRIO, Warsaw 2009, s. 64.

[32] See more in: R. Miętkiewicz, Bezzałogowe platformy morskie. Bezzałogowe jednostki nawodne, Wyd. AMW, Gdynia 2018.

activity at sea – an attack using flying drones[33] on the tanker MT MERCER STREET[34] (sailing from Dar es Salaam in Tanzania on 21 July and bound for Fujairah in the United Arab Emirates). As a result of this attack, an explosion was triggered on board the ship with a crew of 27.[35] Two people were killed in the attack - the captain, a Romanian national, and a British crew member. From a global perspective, as pointed out by S. Kalitowski, 'the risk profile for merchant ships crossing the Persian Gulf, the Gulf of Oman, the Arabian Gulf and the Red Sea remains high, and there is no doubt that the threat in the area to ships engaged in shipping is high, and the possibility of crew members detecting a drone attack is low, as is the possibility of countering a UAV carrying an explosive payload, since merchant ship crews are currently not equipped with radar, sonar, jammers or neutralizers, all of which are expensive devices that are unlikely to be found on board ships, even if there is a need for it."[36]

On the other hand, if we look at the Baltic Sea area – the Maritime Doctrine of the Russian Federation, promulgated and signed by decree on 31 July 2022, includes a provision of one of the 14 most important national interests of the Russian Federation in the World Ocean, i.e., "Safe operation of offshore pipeline systems for the transportation of hydrocarbons".

It is also important to note that drones serve their purpose both ways – to gain an advantage, i.e., hostile use, and they can be used to develop CI resistance.

## Surface and underwater drones – security/defence potential

Faced with the expansion of NATO to include Sweden and Finland and the consequent 'conversion' of the Baltic Sea to a North Atlantic Treaty Area, it should be accepted that this relatively shallow body of water may become an arena for hostile operations - sabotage, information warfare, cyber warfare, the introduction of disinformation, false alarms or warnings that will put forces on alert, concentrating them in a particular location and thus separating them from concurrently ongoing tasks. Intentional, unlawful attacks at sea and in ports against ships, cargoes in transit, crews, passengers, port facilities and maritime and coastal installations remain a challenge. In the 21st century, unmanned platforms and autonomous vehicles are elements that do not require the active participation or official involvement of non-state actors.

It should be noted that another section of the national border in the north of Poland has recently received special attention.

[33] Part of the nearly century-long "Shadow War" between Israel and Iran.

[34] MT MERCER STREET is an oil tanker that sails under the flag of Liberia and has a Japanese owner. It is operated by Zodiac Maritime, the London-based company owned by Israeli Eyal Ofer, a billionaire, real estate and shipping magnate and philanthropist.

[35] Consisting of Romanian, Russian, Chinese, Ukrainian, Filipino, Georgian and Indian nationals.

[36] S. Kalitowski, Ataki na statki z wykorzystaniem dronów na podstawie ataku na MT MERCER STREET, accessed online: http://maritime-security.eu/artykuly/ataki-na-statki-z-wykorzystaniem-dronow-na-podstawie-ataku-na-mt-mercer-street/ (21.05.2024).

Hence, the leading role needs to be given to raising one's own awareness of both potential and actual threats. Indeed, the focus in recent years has been on securing CI on land and in the air. There have been numerous discussions regarding the use of new technologies to monitor security around these environments, especially in terms of building anti-drone systems. However, the maritime area belonging to a seaside state of Poland with a coastline of 770 km, internal waters covering 2,005 km$^2$, the territorial sea extending to 8,682 km$^2$ and the EEZ covering 22,500 km$^2$ and the maritime border of 500.94 km (12.5% of the entire Polish border) remains neglected in this respect.

The dynamic development of unmanned platforms (systems) represents a double-edged weapon of sorts. The use of unmanned/autonomous technologies in the area of maritime security is a highly topical issue. Aerial platform technologies are well advanced and leading the way. However, concerning maritime drones, both surface and underwater, there are still many possibilities to explore. It is necessary to draw on domestic achievements and complement the capabilities of services dedicated to protection and defence with the achievements of private companies, research centres and the potential of students attending technical universities.

As indicated previously, protection against threats requires, e.g., the LNG terminal in Świnoujście, which plays a key role in diversifying supplies of the commodity of strategic importance for the state's energy security. In view of the high hopes surrounding the launch of the Baltic Pipe, which is perceived as an investment of fundamental importance for Poland, it would be worth concentrating efforts on securing this key infrastructure. Ensuring the safe operation of this facility is of particularly high national and even international importance. The possibility of detecting a threat to shorten the path in terms of 'disclosure-response' undoubtedly makes it possible to implement modern solutions, automated bodies, and highly developed technologies. Today, systems utilizing state-of-the-art autonomous technologies increasingly ensure the effective functioning of the critical infrastructure protection system. Among the most significant benefits are the ability to carry out uninterrupted monitoring - whether in air, surface or underwater environments - and the ability to counter identified threats as soon as their symptoms are detected. Such a solution shortens the time between the detection and classification of threats and their counteraction.

Protection against unmanned surface and underwater platforms requires modern detection and neutralisation systems (sonar, radar systems, and signal jamming systems). The development of anti-drone technology remains of utmost importance in this regard.

At this point, it is worth reflecting on the security of underwater communication cables. "Security-oriented operations in this area include not only physical measures such as maritime patrols or monitoring systems but also advanced cyber-security solutions to protect against hacking attacks and other forms of cyber threats."[37] It is crucial to note that "strategically, maintaining the integrity and security of underwater communication cables

[37] R. Dmochowski, Strategiczne fundamenty bezpieczeństwa morskiego…

is also significant in terms of maintaining geopolitical stability, as damage to or loss of access to these structures can have significant consequences for the balance of power in the international arena. Protecting underwater communication cables in the digital age is a task of strategic importance, requiring an integrated approach combining technology, military tactics and cyber security strategies to ensure the continuity of global data exchange and the maintenance of information security."[38] Here, in the depths of the sea, the key role of highly advanced technology, in the form of remotely operated or autonomous underwater vehicles (ROVs/AUVs), must be acknowledged.[39]

Drones, in their ambidextrous nature, can prove useful for monitoring the marine environment. This involves both the detection of potential intentional threats (e.g., posed by foreign services) or beyond these anthropogenic threats, as well as technical threats (e.g., pollution caused by the release of substances) and natural threats (caused by natural forces). Their potential to reach places where conventional access is not possible or is very difficult for a variety of reasons should be exploited. The value of drones in the context of supporting search and rescue operations or delivering humanitarian aid needs to be recognised.

However, it should be taken into account that the use of drones requires having (and strict compliance with) the relevant permits.

## CONCLUSIONS

In the author's opinion, traditional methods of protecting maritime and port infrastructure are insufficient in the face of new threats caused by the developing technology of unmanned platforms (surface, underwater, flying). Rapidly evolving drone technology requires continuous adaptation of measures to protect infrastructure critical to state security. Countering and combating threats in the maritime domain, due to the complexity of the environment and the multifaceted nature of the dangers, is specific and heterogeneous, which implies the need to constantly seek new solutions.

The primary risk that leads to others is negligence. For years, many experts have highlighted the neglect of protection and security in the maritime sector, including the importance of preparing and equipping the relevant forces responsible for this area.. Poland's position by the Baltic Sea has not been fully utilized, partly due to an ambivalent attitude toward maritime issues and a focus on viewing Poland primarily as a continental country. This has resulted in a lack of development of maritime forces, including the capabilities of the Polish Navy.. This is a significant oversight, as the maritime environment is not free from impending threats..

[38] Ibidem.

[39] Such resources are only available in a few EU Member States. This could be promoted by the development of the HERMES project (for the study of European marine ecosystems at the continental boundary), which strongly emphasises the coordination of the extensive infrastructure of European maritime institutions and the development of advanced drone technology to study deep-sea ecosystems and the well-being of the unknown species that inhabit them, in order to develop plans for the sustainable management of these most fragile and mysterious resources of the Old Continent. See more in: European scientists peer into the abyss, accessed online: https://cordis.europa.eu/article/id/23677-european-scientists-peer-into-the-abyss (01.06.2024).

Particularly the Baltic Sea, which harbours sunken chemical munitions.[40] The Baltic Sea is crucial for the security of the Republic of Poland, featuring important and thriving ports as well as offshore installations. It is home to the LNG terminal in Świnoujście, and plans are in place for an FSRU unit to be established near Gdańsk. Additionally, the Baltic Sea is seeing significant investments in offshore wind farms and nuclear power plants.

Even listing the above-mentioned facilities, one can imagine the repercussions caused by a security breakdown in the maritime environment. Threats in the *maritime safety* area include environmental safety, navigational safety, port safety and other elements of maritime CI.

Ports and offshore installations, the planned investments serve to increase the security and diversification of natural gas supplies and to create competitive gas markets in Central Europe and across the Baltic region. Considering the importance of key areas, it remains vital to ensure the best possible protection against actual and potential threats. ”The extent of damage, casualties, economic losses and the political and propaganda overtones of the terrorist attacks on offshore facilities that have been carried out so far[41], show what an effective weapon they are in the hands of terrorists (…).”.[42]As far as maritime areas are concerned, terrorism raises economic issues affecting maritime communications and energy security (gas pipelines, pipelines, oil platforms). Recent events (attacks on NS1 and NS2, incidents reported by the services of the Kingdom of the Netherlands and the Kingdom of Belgium) demonstrate that elements of maritime critical infrastructure face serious threats. Taking into account one of the biggest threats in the risk assessment, i.e., terrorism (also in the maritime area), it should be noted that sabotage and diversionary activities may occur alongside incidents of a terrorist nature.

The effectiveness of protection against actual and potential threats depends on the implementation of appropriate legal regulations and uninterrupted cooperation between the various actors involved. Adequate legislation should allow coordination between different types of actors (institutions and services). The discussed threats should be reflected in the CI protection (CIP) plans, especially in times of the amendment of the Crisis Management Act[43] and the implementation of the CER Directive into the Polish legal order.[44] Currently, there are no criminal sanctions for operators who disregard the obligation to have an approved CIP plan.[45] The CER Directive requires EU member states to establish an entity to serve as the national auditor. CIPs should be updated on a regular basis.[46] A risk

[40] See more in: J. Michalak, Bezpieczeństwo morskie państwa…

[41] See more in: D. Olender, Terroryzm morski…, op. cit., p. 65-67, 120-122.

[42] W. Drewek, Zagrożenia i problemy w transporcie gazu ziemnego drogą morską, ”Logistyka – nauka” 2011, No. 5, p. 523-532.

[43] Act amending the Act on crisis management and certain other acts (Draft dated 03.07.2024 version - interministerial consultation).

[44] Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ EU L 333/164 of 27 December 2022).

[45] And a number of other guidelines contained in the National Plan for the Protection of Critical Infrastructure.

[46] Notwithstanding the calls for their abolition and replacement by appropriate documentation – the changes should be considered in the context of the status as it stands today, and today's NPPCI obliges the relevant actors to develop, approve and implement CIP plan.

analysis and assessment, together with the anticipated development scenario, should be based on current and foreseeable undesirable situations. The documents must detail any potential risks and the assumed preventive and mitigating measures. The plans should reflect the real effort to develop and deploy CI protection. A well-executed planning process enhances an entity's ability to detect and identify threats, minimize vulnerabilities, and effectively counter and respond to incidents, reducing their overall impact. In addition, plans should be reviewed in the light of progressive developments at least once every six months, taking into account emerging technologies (risk matrix). The conflicts we face will not lose their hybrid character, and in doing so, the achievement of the objectives of the operations conducted will be underpinned by the improvement of current technologies and the introduction of innovative technological developments (autonomous systems). Unfortunately, as of now, there are no security standards for any infrastructure that is not on land.

Given the development of the offshore initiatives, it would be advisable to intensify activities aimed at securing the maritime area. In recent years, the focus has shifted to securing CI in the land, air domains. The use of new technologies to monitor security in the vicinity of these environments is frequently discussed, especially in terms of building anti-drone systems. However, the maritime area remains neglected in this respect. The synergic use of both airborne and maritime (surface and underwater) unmanned systems can enhance the safety of infrastructure facilities.

**Literature:**

**Legal acts, reports, strategy documents**

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345/75 of 23 December 2008),

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ EU L 333/164 of 27 December 2022).

Council Regulation (EU) 2022/2474 of 16 December 2022 amending Regulation (EU) No 833/2014 *concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine* (OJ L 322 I of 16 December 2022).

*Act of 26 July 2007 on crisis management* (Journal of Laws 2024, item 834).

*Act on amending the Act on crisis management and some other acts* (draft dated 03.07.2024 version - interministerial consultations).

Annex to the announcement of the Speaker of the Sejm of the Republic of Poland of 14.07.2023 - *Act of 20 December 1996 on seaports and harbours* (Journal of Laws of 2023, item 1796).

**Non-serial publications**

Dougherty M.J., Drony. Ilustrowany przewodnik po bezzałogowych pojazdach powietrznych
i podwodnych, Wyd. Bellona, Warszawa 2015.

Jędrzejewski W., Terminal LNG w Świnoujściu a integracja środkowoeuropejskiego rynku gazu [in:] Piątek J.J., Podgórzańska R. (ed.), Terminal LNG w Świnoujściu a bezpieczeństwo energetyczne regionu i Polski, Wyd. Adam Marszałek, Toruń 2013, p. 17-30.

Konkol D., Perka T., Polskie porty morskie, Dom Wydawniczy Księży Młyn, Łódź 2011.

Kubiak K., Przemoc na oceanach. Współczesne piractwo i terroryzm morski, Wyd. TRIO, Warszawa 2009.

Łukasiewicz J., Bezzałogowe statki powietrzne jako źródło zagrożeń infrastruktury zaopatrzenia państw w energię elektryczną oraz proponowane metody ochrony tej infrastruktury, ”Terroryzm. Studia, analizy, prewencja” 2022, No. 1 (1), Wyd. Agencji Bezpieczeństwa Wewnętrznego, p. 90-122.

Michalak J., Bezpieczeństwo morskie państwa wobec zagrożeń generowanych przez zatopioną amunicję chemiczną, AMW, Gdynia 2018.

Miętkiewicz R., Bezzałogowe platformy morskie. Bezzałogowe jednostki nawodne, Wyd. AMW, Gdynia 2018.

Olender D., Działania Policji w zakresie ochrony przed terroryzmem nowo powstającego terminalu LNG w Świnoujściu [in:] Bezpieczeństwo. Zagadnienia, K. Kraj (red. nauk.), WSIiZ, Rzeszów 2013, p. 79-92.

Olender D., Terroryzm morski – przeciwdziałanie i zwalczanie, Wyd. ASzWoj, Warszawa 2018.

Szubrycht T., Morskie aspekty międzynarodowego terroryzmu (in:) M. J. Malinowski,
R. Ożarowski, W. Grabowski (ed.): Ewolucja terroryzmu na przełomie XX i XXI wieku, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2009.

Wyszywacz W., Drony, Wyd. II rozszerzone, Wyd. Poligraf, Brzezia Łąka 2020.

**Articles in periodicals**

Drewek W., Zagrożenia i problemy w transporcie gazu ziemnego drogą morską, ”Logistyka – nauka” 2011, No. 5, p. 523-532.

Hypki T., Atak na rurociągi Nord Stream 1 i 2, ”Raport. Wojsko, technika, obronność” 2022, No. 10, p. 4-9.

Hypki T., Wojny bezzałogowców, ”Raport. Wojsko, technika, obronność” 2022, No. 11,
s. 4-12.

Olender D., Gazoport w Świnoujściu jako potencjalny cel terrorystów, Zeszyty Doktoranckie Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej” 2013, nr 3(8), Warszawa 2013, p. 74-85.

**Online sources:**

Dmochowski R., Strategiczne fundamenty bezpieczeństwa morskiego (analiza), accessed online: https://portalstoczniowy.pl/strategia-

fundamenty-bezpieczenstwo-morskie-ochrona-infrastruktura-krytyczna-globalny-system/ (01.06.2024 r.).
European scientists peer into the abyss, accessed online: https://cordis.europa.eu/article/id/23677-european-scientists-peer-into-the-abyss (01.06.2024 r.).
Granice RP, accessed online: https://www.strazgraniczna.pl/pl/granica/granice-rp/1910,Granice-RP.html (21.05.2024 r.).
Jakóbik W., Opracowanie: Gazoport w Świnoujściu wpłynie na rynek w Europie, projekt w Kłajpedzie jest kluczowy głównie dla Litwy, accessed online: http://jagiellonski.pl/?p=3022 (12.04.2016 r.).
Kalitowski S., Ataki na statki z wykorzystaniem dronów na podstawie ataku na MT MERCER STREET, accessed online: http://maritime-security.eu/artykuly/ataki-na-statki-z-wykorzystaniem-dronow-na-podstawie-ataku-na-mt-mercer-street/ (21.05.2024 r.).
Maritime boundaries between Denmark and Poland, IILSS – International Institute for Law of the Sea Studies, accessed online: http://iilss.net/maritime-boundaries-between-denmark-and-poland/ (21.05.2024 r.).
Over 40 years of conflict is over: Denmark & Poland agree on border, accessed online: https://energywatch.com/EnergyNews/Policy___Trading/article10981245.ece (21.12.2022 r.).
Poland and Denmark sign agreement on maritime boundary in the Baltic Sea, accessed online: https://maritime-spatial-planning.ec.europa.eu/events/poland-and-denmark-sign-agreement-maritime-boundary-baltic-sea (21.05.2024 r.).
Program rozwoju Morskich Farm Wiatrowych, accessed online: https://www.gov.pl/web/morska-energetyka-wiatrowa/program-rozwoju-morskich-farm-wiatrowych (31.05.2024 r.).
Russian Aircraft Conduct Unsafe, Unprofessional Overflight of NATO Ships in Baltic Sea, accessed online: https://mc.nato.int/media-centre/news/2022/russian-aircraft-conduct-unsafe--unprofessional-overflight-of-nato-ships-in-baltic-sea (19.05.2024 r.).
World's LNG Liquefaction Plants and Regasification Terminals, accessed online http://globallnginfo.com/GLNG_Database.aspx (01.05.2024 r.).
www.icao.int/Pages/default.aspx (20.05.2024 r.).

# BEZZAŁOGOWE PLATFORMY NAWODNE, PODWODNE JAKO NOWE WYZWANIE I ZAGROŻENIE DLA MORSKIEJ I PORTOWEJ INFRASTRUKTURY KRYTYCZNEJ

**Streszczenie:**

W ostatnim czasie coraz częściej można usłyszeć o zagrożeniu, jakie stanowią bezzałogowe platformy dla bezpieczeństwa państwa. Zapewnienie ochrony przed tego rodzaju zagrożeniami stanowi coraz większy zakres w planowaniu ochrony obiektów infrastruktury krytycznej. Jest to o tyle istotne, że na chwilę obecną brak jest standardów w zakresie bezpieczeństwa, w tym informacyjnego, dla jakiejkolwiek infrastruktury, która nie jest na lądzie. Z uwagi na ograniczenia objętościowe wynikające z charakteru publikacji, Autor skupił się na wybranych aspektach prezentowanego zagadnienia. Jednak osiągnięcie tego celu wymagało znalezienia odpowiedzi na trzy pytania pośrednie dotyczące wyzwań związanych z funkcjonowaniem infrastruktury morskiej, zdefiniowania zagrożeń ze strony dronów nawodnych i podwodnych oraz wskazania działań ukierunkowanych na zapewnienie ochrony w przedmiotowym zakresie.

**Słowa kluczowe:** bezpieczeństwo, ochrona, bezzałogowe platformy, nawodne i podwodne platformy, drony, sabotaż, infrastruktura krytyczna.