#GIDSstatement 5 / 2025

Michał Piekarski

Maritime Critical Infrastructure and Lessons from the Black Sea: Hybrid Threats from Russia to NATO's Littoral States on the Baltic Sea

Observations from Poland, a frontline state

#GIDSstatement | No. 5 / 2025 | April 2025 | ISSN 2699-4372

The present article is one of several working papers resulting from a workshop conducted prior to the 2024 Kiel International Seapower Symposium on the topic 'Re-Learning War: Lessons from the Black Sea'. The workshop was co-hosted by the GIDS and the Institute for Security Policy at Kiel University (ISPK) on 20 June 2024. The topic of each paper was discussed during the workshop. All articles have been peer-reviewed and will also be published in the ISPK's 'Policy Brief' format.

GIDS GERMAN INSTITUTE FOR DEFENCE AND STRATEGIC STUDIES

The German National Library lists this publication in the German National Bibliography; detailed bibliographic information is available online at http://dnb.dnb.de

ISSN 2699-4372

This #GIDSstatement is published by the German Institute for Defence and Strategic Studies (GIDS) – Directorate Strategic Studies and Research (DSSF).

Contributions are available free of charge from the GIDS website: www.gids-hamburg.de

#GIDSstatement reflects the personal opinions of the authors and does not necessarily represent

Proposed citation:
Michał Piekarski, Maritime Critical Infrastructure and Lessons from the Black Sea: Hybrid Threats from Russia to NATO's Littoral States on the Baltic Sea. Observations from Poland, a frontline state, #GIDSstatement 5/20025: Hamburg.

GIDS
German Institute for Defence and Strategic Studies
Bundeswehr Command and Staff College
Manteuffelstraße 20 · 22587 Hamburg, Germany
Tel.: +49 (0)40 8667 6801
buero@gids-hamburg.de · www.gids-hamburg.de

Dr Michał Piekarski*

Maritime Critical Infrastructure and Lessons from the Black Sea: Hybrid Threats from Russia to NATO's Littoral States on the Baltic Sea

Observations from Poland, a frontline state

Poland is already exposed to hybrid attacks from Russia and actors supported by Russia.[1] These attacks take various forms: Apart from the ongoing crisis on our border with Belarus, there have been several attempts to conduct acts of sabotage against critical infrastructure and a number of other incidents that are still not fully explained. We also know of intelligence activities and disinformation campaigns. Against this backdrop, the following questions arise: What are possible scenarios of hybrid warfare in the Baltic Sea and what key lessons can we learn from the Ukraine War? What measures can be taken to increase maritime security in the Baltic Sea region?

This paper seeks to answer these questions and provide recommendations for action. To this end, examples of hybrid threats and several scenarios – or warnings – will be described.

1 General Lessons and Russian Potential

Pre-2022 data regarding the naval potential of Russia and Ukraine would show that, even when counting only Russia's Black Sea Fleet, the aggressor had a clear advantage over the defender – especially if one looked at the plain numbers of vessels, aircraft, and shore-based forces. The outcome of the naval battle seemed to be decided even before the first shots were fired.

However, to this day Russia has already lost at least nineteen ships of various classes, including the Moskva cruiser and two modern missile corvettes. Russian forces have been proven weaker than anticipated. The Ukrainian efforts – drone and missile strikes – have to some degree levelled the playing field, limiting Russian operational freedom on the Black Sea and causing damage to ships and shore facilities.

On the other hand, Russian actions have inflicted considerable damage on Ukraine. For example, ships and submarines have been used to launch cruise missiles, targeting

* Dr Michał Piekarski is Assistant Professor at the Institute of International and Security Studies at the Faculty of Social Sciences of the University of Wrocław. His research focuses on national security issues, particularly hybrid threats, maritime security, and Poland's strategic culture.

1 For example, in 2024 nine people who had planned an arson attack on a chemical plant in Wroclaw were arrested and charged with espionage and sabotage (Ptak 2024). In 2023, a group of people who had gathered intelligence on railway lines and were preparing to derail trains were arrested (Associated Press 2023). In addition, the border crisis with Belarus continues.

Ukrainian cities and critical infrastructure. The Russian naval blockade caused significant economic problems to Ukraine leading to wider consequences.[2]

Therefore, one lesson to be drawn is: even if a war is land-centric and air-focused, the maritime domain still matters.

Successful Ukrainian attacks, including drone and missile strikes, have shown that Russian forces have exploitable vulnerabilities. Their anti-access/area denial (A2/AD) zones created by missile systems – sometimes colloquially described as 'bubbles'[3] – can be burst, and drone attacks were apparently a surprise for Russian forces, revealing inadequate force protection against such attacks.

Yet despite the losses in the Black Sea, Russia still possesses notable naval resources. For example, most of its Baltic Fleet remains intact.

According to 'The Military Balance', in 2023 the Baltic Fleet possessed one submarine, one guided missile destroyer, seven frigates and thirty-five smaller surface combatants and patrol vessels as well as twelve mine warfare ships and thirteen amphibious vessels.[4]

However, this data does not consider other elements of the Russian forces. Apart from its aviation component and shore-based forces, including naval infantry, special operations forces, and coastal missile batteries, Russia has other tools at its disposal. One is the paramilitary component – like the border guard, subordinate to the Federal Security Service (FSB). Another set of tools are formally civilian ones. One is the state agency named Main Directorate of Deep-Sea Research, which operates a fleet of surface and submarine research vessels that may be used to gather intelligence or conduct sabotage.[5] Another refers to commercial vessels including the so-called 'shadow fleet' – owned by shell companies, often without direct links to Russia.[6] Apart from operating alone or in conjunction with military special operations forces, they could also be utilised in hybrid warfare activities – for instance, if Russia wishes to keep a conflict below the threshold of open, conventional war.

Overall, it is clear that the Russian forces have strengths and weaknesses and that Ukraine has been able to exploit some of these weaknesses by conducting successful missile and drone strikes. On the other hand, Russia is still able to launch missiles using various platforms, including maritime ones. Therefore, when assessing the general Russian potential and looking at Black Sea naval engagements as a source of 'lessons learned', one aspect is particularly important with regard to the Baltic Sea. In this theatre, both NATO and Russia have advantages and disadvantages, for instance due to geographic conditions. For example, in case of open war, the Russian bases in Kaliningrad could be targeted by the Polish Coastal Missile Unit, which is armed with NSM cruise missiles; and port facilities as well as moored ships could be attacked by the Polish Land Forces and their HIMARS launchers. Therefore, a repetition of the successful attacks on ships in the Black Sea would be possible in the Baltic setting. In the Russo-Ukrainian

2 For example, grain that could not be exported via the Black Sea route was either sold in Poland or rerouted to Polish ports. The influx of grain resulted in protests of Polish farmers and there is suspicion that at least one act of sabotage targeting a grain-carrying train was committed involving Russian-supported persons.
3 Dalsjö et al. 2019.
4 IISS, The Military Balance 2024.
5 Kaushal 2023.
6 Braw 2024.

war, Russian air defence systems have been unable to provide sufficient protection against drones, cruise missiles and tactical ballistic missiles that represent a fraction of NATO capabilities – and it is safe to assume that a greater number of assets could be successfully deployed in Baltic area.

However, another important question arises with a view to Russia's possible and probable course of action.

Since the Russian fleet already has a number of ships armed with cruise missiles, and has missiles at its disposal that can also be fired from land and air platforms, Russia could carry out a pre-emptive or retaliatory strike against Polish ports and other infrastructure, both military and civilian. Furthermore, hybrid warfare scenarios provide even more dilemmas and questions. In comparison to conventional warfare, which would lead to the invocation of Article V of the North Atlantic Treaty and the deployment of at least part of available NATO forces, hybrid warfare may allow Russia to keep the crisis below the Article V threshold and try to achieve its political goals while limiting the risk of a conventional confrontation with NATO.

2 Potential Role of Russian Naval Forces in a Hybrid Conflict

Russian naval forces could be utilised in several ways during a potential conflict. As described above, hybrid warfare, defined as actions occurring close to the threshold of open warfare, is one potential way of operation. In the maritime domain, the spectrum of possible hybrid actions stretches from intelligence gathering, show of force, and testing the other side's defence mechanisms to sabotage. Certainly, intelligence gathering is constantly conducted. It involves not only traditional activities using naval vessels or aircraft, but also civilian ships. They may be used to gather information on shipping, ports, and critical infrastructure (like pipelines). For example, in 2023 two freighters were noticed loitering close to Polish territorial waters without a clear purpose.[7] The purpose may well have been to gather intelligence or to test the response and reaction time of Polish authorities.

Another form of aggressive action is the well-known harassing ('buzzing') of ships by Russian ships and aircraft. While such behaviour is not a direct attack, it involves a high risk of accidents and may be used in information warfare. For example, one buzzing incident was used to spin a narrative about Russia's purported ability to deactivate a ship's electronics systems.[8] That narrative represents a typical case of spreading disinformation. Other recent cases of navigation systems jamming represent a different form of harassing where an actually existing capability is employed to threaten the general safety of shipping and aviation.[9]

Another imaginable scenario is the attempt to weaponise certain cases or issues. In May 2024, a draft document was posted online by the Russian government. According to this document, Russian maritime borders in the Baltic Sea region may be revised or even changed, under the pretext that the territorial waters off Russia's mainland coast were measured in 1985 on the basis of 'small scale nautical navigation maps'[10]. While

7 Marszałkowski 2023.
8 Meurmishvili 2017.
9 Eggert 2024.
10 Associated Press 2024.

this incident is enigmatic, it is possible that it was designed to test the response of the Baltic neighbours. If Russia proceeded with this course of action and tried to unilaterally change maritime borders, it could use its border guard force for the first steps – as in May 2024, when the Russian border guard removed buoys marking the border with Estonia on the Narva River.[11]

There are even more possibilities for Russia acting on the basis of unilateral interpretations of legal rules and claiming that certain measures are necessary for reasons of shipping safety. For example, part of the Polish EEZ overlaps with Russia's declared search and rescue region. This could potentially be weaponised by Russia creating a crisis followed by unilateral action under the cover of a 'rescue mission' or 'antiterrorist operation.' Such a pretext would be paper thin but could be a justification for the deployment of forces.

Beyond that, another possible set of action has to be highlighted. It refers back to events such as the damage to the Nord Stream and Baltic Connector pipelines as well as GPS jamming cases. These represent attacks on maritime critical infrastructure, which consist of several elements:

— **Transportation systems**: ports, ships, and aids to navigation. The Polish ports in Gdańsk, Gdynia and Szczecin-Świnoujście are critical to the economy and ensure strong trade relations. According to official data, in 2023 annual cargo tonnage in Polish seaports reached 135.9 million tonnes (for comparison: in 2022 it was 119 million tonnes).[12] In 2024, the amount of cargo traffic was slightly lower – 135 million tonnes.[13] The most important types of cargo are liquid fuels, bulk cargo, and containers. The port of Gdańsk is particularly important for this last type of cargo, having constantly exceeded the number of 2 million TEUs since 2021.[14] A further increase in cargo handling is also expected in Szczecin-Świnoujście and Gdynia due to the planned expansion of these ports, including the construction of new container terminals. Therefore, limiting or stopping cargo traffic always creates the risk of causing significant economic disruptions and breaking supply chains. Poland also has naval and law enforcement (Border Guard) bases, providing capabilities to receive allied military support in the event of a crisis. In this respect, the consequences of disruption may be severe, particularly if a port is forced to limit or suspend operations. Compensating for this loss of capacity would be challenging for other ports.

  Additionally, these ports play a crucial role in energy security. Poland's only LNG terminal is located in Świnoujście harbour, and the port of Gdańsk, which is already equipped with a large oil terminal, is going to be expanded to include a Floating Storage Regasification Unit (FSRU).

— **Energy-related infrastructure:** pipelines, energy cables, and offshore platforms. Until recently, the latter were just oil platforms – but due to the developments in offshore wind generation, the importance of these installations is expected to increase rapidly. According to current Polish government policy

11 Hartog 2024.
12 GUS 2024.
13 Trade.gov.pl 2024.
14 Port Gdańsk 2024.

documents[15], Poland is reforming its energy policy. Traditional energy sources like coal or Russian-supplied gas and oil are being replaced by other sources. Therefore, any disruption may bring serious consequences for society and the economy alike. For example, as far as gas is concerned, the main import routes are maritime ones: by the Baltic Pipe and LNG terminals. Any attack on those facilities would very likely result in limiting the supply of natural gas, which is critical for industry and households. That would require taking alternative steps: rationing energy use, employment of emergency gas reserves and searching for alternative routes of supply. Even in case of a short disruption, it is expected that Russian information operations would portray this as a much more serious incident – and try to create panic and fear among the population. Therefore, ensuring the security of those energy import routes is critical.

— **Communication infrastructure:** undersea data cables. These may be targeted in order to intercept data or disrupt online services and data transfer. While the interception of data is a typical activity in the signals intelligence field and does not cause publicly visible immediate harm, the disruption of the flow of data may be useful for Russia since it affects the availability of online services and information, and this, in turn, may create a permissible environment for (dis)information campaigns. Certainly, such an operation would be most effective if other communication infrastructure (land and satellite connections) were targeted.[16]

All the assets mentioned above can be targeted in various ways; scenarios can be classified by probability. The most unlikely scenario is an early overt Russian action – this would constitute an armed attack and could trigger Article V of the NATO treaty, which may not be desirable to the aggressor. It is much more likely that an attack would be carried out in a way that allows it to be kept below an escalation threshold. Such an attack could be a highly ambiguous action, staged to look like an accident. The 'anchor dragging' that damaged the Baltic Connector is one notable example, as are the later cases of the vessels Eagle S and Yi Peng 3, which are suspected of damaging several data cables in the Baltic Sea.[17]

Another possibility would be the blockade of a major port, for instance by civilian vessels. For example, a freighter might enter the port for a legitimate reason and later cause a collision with another ship or port infrastructure, or sink for some other pretend reason. This would block entry to and exit from the harbour, disrupt port operations and require a long and costly effort to salvage the vessel. At the same time, the consequences would be noticeable. Such an attack, if conducted during a major crisis, could effectively limit the amount of military equipment that could reach Poland in time.

An attack masqueraded as a 'protest action', such as a port blockade by yachts and other small civilian boats, would also be a possibility. That form of protest could target ships transporting military equipment or oil and gas tankers. Other potential targets could be LNG terminals, such as the FSRU that is planned to be constructed near

15 The most relevant are: Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (*National Security Strategy of the Republic of Poland*) (2020) and Polityka energetyczna Polski do 2040 r (*Energy Policy of Poland until 2040*) (2021).

16 Murphy et al. 2016; Lange et al. 2019.

17 Wiese Bockmann 2024.

Gdańsk. The action could be disguised as an ‘anti-war’ or ‘ecological’ protest and, if the blockade is lifted by force, a narrative could be spun around a violent regime that disregards the citizens’ right to protest.

More advanced and more kinetic methods may include the covert mining of shipping lines, ports and anchorages or acts of underwater sabotage. Also, the use of other means is conceivable. For example, unmanned surface or aerial vehicles could be used to attack critical infrastructure. In these scenarios, the actions of a state actor (Russia) would be disguised as activities of non-state actors – such as terrorists or protesters. Hypothetically speaking, acts of sabotage at an LNG terminal could be disguised as actions by violent environmental activists.

Finally, it is sensible to consider the possibility of an overt military operation, as the final element in a string of hybrid actions. Following an at least partial disruption of critical infrastructure, increasing polarisation of society, and actions that would undermine Allied unity, a short-term, limited use of force could be employed to pressure Poland into complying with Russia’s will. An example would be a single cruise missile attack on oil refineries or power plants. This would be an ‘escalate to de-escalate’ scenario.[18]

All these scenarios show that an important element of hybrid warfare is the combined use of different elements. All actions would be interlinked, different tactics and tools would be mixed to destabilise Poland’s society and economy, create polarisation and shape the security environment according to Russia’s wishes. The last element could be the open use of force, as illustrated by the last scenario.

3 Recommendations for Security Policy in the Baltic Sea Region

This part of the paper focuses on possible measures to prevent or respond to hybrid activities. These recommendations and conclusions are written from a Polish perspective, but may also be applicable to other countries of the region. The conclusions range from general ones, related to wider policy and strategy issues, to more specific ones associated with technical capabilities and the procurement of certain platforms.

3.1 Tackling sea blindness

One of the fundamental recommendations is to limit ‘sea blindness’ – the lack of awareness related to maritime (security) issues. This is particularly important in the context of critical infrastructure protection, as problems different from those encountered in the land domain mean that techniques, tactics, procedures and equipment typically used on land may not be applicable to protect offshore wind farms or pipelines, particularly outside a country’s territorial waters. This understanding is fundamental for the further recommendations described below, especially for the formulation of a strategy to prevent and respond to Russian activities. Therefore, continuous informational and educational efforts aimed at both the general public and decision makers are recommended.

This is imperative, given the fact that the Baltic Sea was not a scene of decisive naval engagements in the 20th century and that there is thus a tendency to consider this area as insignificant. This, in turn, leads to the setting of different priorities in security

18 A more detailed discussion of similar scenarios can be found in: Frederick et al. 2022.

policy, with a special focus on the land domain. Notably, the role of the Baltic being important not only for security and defence, but also for commercial shipping and energy generation and transfer should be constantly explained to the public and decision makers alike.

3.2 Formulation of a strategy and implementation at the operational level

Key areas of maritime security and related recommendations need to be translated into a national-level strategy. Ideally, such a maritime security strategy should describe the key national interests in the Baltic Sea area. The strategy should also define an area of responsibility – either only the Southern Baltic Sea (territorial waters and EEZ) or additional areas as well (the rest of the Baltic, the Danish Straits, the North Sea or others), based on which areas are considered important and where Polish forces should be deployed.

However, a more specific document should directly describe the strategic interests and objectives as well as the measures taken to prevent and respond to crisis situations and threats in the Baltic Sea region. In the Polish hierarchy of strategic documents, this would ideally be a document published by the Ministry of Defence, i.e. one level below the National Security Strategy.

There should be a clear plan of action, particularly for crisis situations that might, at least initially, lie below the threshold of an armed conflict. Specifically, the strategy should describe the desired approach to deterrence. A defensive approach – implemented by building hardened, resilient infrastructure – would be a form of deterrence by denial. Another way could be deterrence through punishment, implemented by imposing sanctions and/or tariffs on Russia in the event of malicious actions in the Baltic Sea area, and by exerting additional political, economic, and military pressure. This path could be more complicated, since it requires ways to apply pressure acceptable under international law, to develop resources that allow credible punishment and, last but not least, to find vulnerabilities that could be exploited.
In any case, the strategy would have to be consistent with strategic decisions made at the NATO level, especially in the context of the recent Washington Summit Declaration.[19]

In addition, such a document should also provide a clear division of roles and responsibilities between various services and organisations. In the case of Poland, it should in particular determine the role of the Navy and the maritime branch of the Border Guard. Currently, the Polish Border Guard is tasked exclusively with law enforcement missions – in the past, it has focused on fishery protection and on countering various forms of smuggling. As a result, it has surface surveillance capabilities (coastal radars, patrol boats, aircraft), but no subsurface surveillance capabilities. It also has a limited capability to engage surface targets, but neither the capability nor the legal basis to engage subsurface targets.

The Polish military, however, is by nature oriented towards countering military threats. Deployment to support the Border Guard is permitted only if civilian resources are deemed inadequate. While this division may be effective in peacetime when attacks on shipping or critical infrastructure are rare, it is less efficient nowadays when, for

19 NATO 2024b.

example, it may become necessary to conduct regular patrolling of pipelines in order to detect sabotage attempts. Under current legal rules[20], however, unless a Navy vessel is deployed as an asset supporting the Border Guard, it is not allowed to perform any law enforcement tasks (such as the boarding and inspection of a suspicious vessel).

Due to the above-mentioned threats, it may be necessary to widen the Border Guard's set of capabilities – including a change of legal rules and investments in more capable equipment – or, alternatively, the consideration of a more active deployment of naval forces. The latter would also require changes to the law and the building or acquisition of more ships to match the requirements. In each case, necessary changes in the legal framework as well as in the organisation, equipment and training of forces should be defined and implemented at the operational level. That is particularly important for shipbuilding and other force generation efforts.

Following the first path to strengthen the Border Guard itself would require changing the rules of engagement, especially in engaging submarine targets and unmanned surface vessels, and the acquisition of new equipment (vessels and aircraft) as well as major changes in training, which would essentially turn the Border Guard into a second Navy.

If we were to choose the second option, naval forces would already have most capabilities at their disposal. From a legal perspective, a standing rule (possibly written into an act of parliament) allowing military personnel to stop, board and inspect vessels both in Polish territorial waters and in its exclusive economic zone as well as new rules of engagement would have to be introduced. Also, military forces would need more vessels and more aircraft, to fulfil their new, widened mission of protecting critical infrastructure.

In the short term, an expansion of the Navy's mission to include the protection of critical infrastructure, which would result in an increase in the size of naval forces, is more promising. The Navy already has the capabilities that the Border Guard lacks – it is easier to enlarge existing forces than to build those capabilities from scratch in a different service.

3.3 Situational awareness

Dealing with hybrid threats means dealing with uncertain situations. Therefore, the ability to achieve and maintain situational awareness is fundamental. This allows not only to detect potential direct threats but also to gather wider intelligence on adversary actions. In the context of hybrid threats, it would be crucial to obtain evidence of potential Russian responsibility and later use this evidence for further (e.g. legal) actions.

In order to maintain situational awareness in the maritime domain, various sensors and resources can be used. From a Polish perspective, all sorts of systems – from land-based radars to sensors mounted directly on or in close proximity to infrastructure to patrol vessels and aircraft – could be employed. What might prove problematic in this respect is that a variety of stakeholders would be involved, from infrastructure owners and operators, maritime administration and law enforcement forces to the military. All of these actors and entities are subject to different legal regulations, and the above-

20 Act of Parliament of the Republic of Poland on State Border Protection (1991) and Act of Parliament of the Republic of Poland on the Border Guard (1990) (with amendments).

mentioned platforms have different capabilities. Another factor is the cost of acquisition and maintenance of surveillance systems, depending on their intended purpose. For example, the most important systems for the owner of an offshore wind farm are those that help to ensure the protection of their property. On the other hand, law enforcement services such as the Border Guard are interested in having systems that fit their law enforcement mission (which currently excludes subsurface surveillance). Finally, the military is interested in having capabilities of detection with regard to a wide range of military threats (including submarines).

Therefore, I recommend to implement integrated surveillance systems – both on the national and international level, if possible. Such systems should receive data provided by the stakeholders mentioned above and could help to establish a common situation picture. An integrated approach should also be the basis for any future developments in this field, also considering shared costs and results. For example, offshore wind facilities could be used as platforms for surveillance systems (radars, cameras or drones).

Finally, critical elements of situational awareness are maritime and airborne intelligence-gathering platforms. The current state of the Polish naval forces and maritime aviation requires the acquisition of new ships and airborne platforms (helicopters and maritime patrol aircraft). The ship-related issues are discussed in more detail below. As for the air domain, it should be noted that a replacement for light patrol aircraft and the procurement of additional helicopters is required. Two Saab 340 Airborne Early Warning planes were acquired in 2023, but they will be required to provide radar coverage also in other areas – notably, on the eastern border with Belarus and Ukraine. A partial solution would be the employment of TB2 and MQ-9B drones in a maritime patrol role; the former have been purchased already, and the latter were ordered recently.

3.4 Ships and shipbuilding

Maintaining situational awareness requires a constant presence, and this presence requires resources – in the maritime domain, these resources are mostly ships. The geography of the Baltic Sea region is one determinant of these requirements. Even if Polish maritime strategy makers decided to limit the area of responsibility to the southern Baltic Sea, vessels would have to be able to remain in the designated areas for a certain period of time while simultaneously detecting and pursuing multiple categories of targets, whether above the surface, on the surface, underwater and on the seabed.

Ships have an additional advantage: the ability to respond to a detected threat, using armament or other capabilities (i.e. a boarding team or special operations soldiers, if they are on board).

For example, in the above-mentioned scenario of a covert mine approach to a port, special mine-countermeasure vessels are the primary tool for detecting and defusing mines. This also illustrates the dual capability that armed forces offer outside of the spectrum of conventional conflict.

In a similar manner, a designated anti-aircraft frigate could be employed to provide protection against airborne threats (such as cruise missiles or drones). The Polish Navy

already has or will have Kormoran II-class minehunters[21] and Wicher-class frigates[22] providing these capabilities. It is important to emphasize that the projected Polish surface fleet shall be composed of three frigates, six minehunters, and one patrol corvette, with the addition of auxiliary vessels and older ships approaching the decommissioning date. Even in peacetime, the tasks of such a small-sized fleet will already be many: training, participation in national and international exercises, deployment to NATO's standing maritime groups and finally planned and unplanned maintenance periods may leave little room for supporting civilian authorities.[23] Therefore, the number of ships may have to be increased, either by upgrading older vessels in order to keep them in service or by purchasing new ships, resulting in higher costs.

The first option is potentially the less costly, but also the more risky approach, since the capabilities of upgraded ships would be limited by their original design. Another unknown factor is how long such ships would be able to remain in service. The second option would be more costly and take more time, since requirements for new vessels would have to be formulated, and the entire acquisition process is complicated. On the other hand, this would provide the Navy with new ships to fulfil its contemporary and future requirements.

Since Poland has not published any official documents regarding naval strategy and shipbuilding plans in a wider perspective besides its Strategic Concept for Maritime Security from 2017, it is difficult to predict how likely the acquisition of new vessels actually is or whether the government might prefer to invest in the retention and upgrading of older ones. However, a telling announcement was made in 2024 regarding the redirection of the 'Murena' (Moray) programme, which was originally aimed at delivering new fast attack craft, towards the acquisition of four multi-role corvettes.[24]

Due to the nature of hybrid threats, it is necessary to consider further procurement projects, including vessels capable of seabed surveillance and underwater activities support (similar in concept to the UK MROSS programme[25]). Given the size of Polish maritime areas and the critical role of seabed infrastructure, notably pipelines and future offshore wind installations requiring underwater power lines, the development of such a capability is crucial. A first step in this direction is the already existing 'Ratownik' programme (for the construction of a submarine rescue and diving support vessel)[26] as well as the planned acquisition of a survey vessel[27].

Another possibility to increase the number of available ships is building dedicated offshore patrol vessels (or patrol corvettes), equipped to detect and counter threats to critical infrastructure and shipping. These vessels should have anti-surface, anti-submarine and anti-aircraft capabilities less advanced than frigates, but most importantly allowing them to detect and respond to enemy unmanned vessels (drones). Their task

21 Six vessels have been contracted. So far, three vessels have been delivered and commissioned into service and a fourth was launched in 2024. Cf. 8th FOW 2024; Wojsko Polskie 2024.
22 Build under the codename 'Miecznik' (Swordfish). Three ships shall be delivered by 2031. See: PGZSW 2024; Wilewski 2023.
23 During the Cold War, when the Polish Navy had many more vessels than nowadays, there were ships deployed on presence / surveillance patrols as well as designated alert vessels, which could be quickly deployed in case of crisis.
24 Kamiński 2024a.
25 Navy Lookout 2023.
26 Kamiński 2024b.
27 Ciślak 2024a.

would be to ensure a presence in the Baltic Sea. This would result in a mixed fleet: a small number of high-end ships for the most demanding missions and a larger number of low-end vessels for simpler tasks. It is possible that the above-mentioned Murena programme may result in the delivery of such capabilities, supplementing high-end guided-missile frigates.

Another fundamental issue that should be the subject of a strategic decision is the maintenance of submarine forces. Currently, the Polish Navy operates one Kilo-class submarine. Regarding the acquisition of new boats ('Orka' programme), it has been announced that submarines shall be purchased and a respective contract shall be signed in 2025.[28] This decision needs to be based on a careful assessment of the Russian threat and capabilities on the one hand, and costs and benefits related to intelligence gathering or special forces support missions on the other. From the Polish perspective, the most important issue is the cost of building and maintaining a fleet, since defence spending is already high due to other projects such as the acquisition of tanks, missile systems for land forces, attack helicopters and air force programmes.

One possible solution would certainly be to increase overall defence spending in order to build more ships, or to redirect funding from air or land programmes to naval ones. From a more realistic point of view, it may be fair to assume that future ship acquisition programmes will be limited, for example to the 'Orca' and 'Ratownik' programmes, which would leave a capability gap. This gap can be covered partially by other systems, especially unmanned ones (drones).

3.5 Drones and counter-drone measures

Due to technical progress and the growing proliferation of unmanned surface and underwater vehicles, it is likely that they may be used as a tool in attacks on shipping or critical infrastructure. However, despite the fact that Russia has employed unmanned surface vessels as a direct response to Ukrainian attacks involving uncrewed vessels[29], a direct replication of activities known from the Black Sea in the Baltic is unlikely, due to the different operational and geographical environment.

Ukrainian surface vessels are usually employed in overt attacks against ships – notably in harbour areas. It is possible that in a hybrid warfare scenario in the Baltic Sea, unmanned underwater vessels would be preferred for several reasons. First, a large number of potential targets are underwater (i.e. pipelines or cables). Secondly, an underwater vehicle is much more difficult to detect. Finally, they are less vulnerable to weather conditions than surface ones. It is known that Russia has developed an autonomous underwater vehicle equipped with a manipulator arm.[30] This Russian construction works just as well on various other vessels. For example, the Russian company Rubin advertises several unmanned systems, named 'Yunona', 'Amulet' and 'Amulet-2' that are easy to transport and deploy without the need to use cranes.[31]

In wartime these unmanned vessels may be employed as part of a system composed of warships, submarines, conventional weapons (missiles) and aircraft. In a hybrid warfare scenario, it is possible that drones in particular could be used in order to enable

28 Ciślak 2024b.
29 Sutton 2024.
30 Sutton 2022.
31 Rubin 2024.

plausible deniability – in this case Russia could use commercially available equipment (entire drones or just their components) and spin the narrative that the attack was carried out by non-state actors.[32]

Therefore, a part of the already mentioned strategy and its operationalisation should be devoted to the establishment of a system aimed at the prevention of and response to malicious drone use. The fundamental issue is to create a legal framework that regulates the use of drones in maritime areas, to establish rules of engagement in the event of a detection of enemy drones, and finally to allocate rules and resources for military, law enforcement and commercial actors. It is simply a matter of choice: if an unidentified drone is detected near a port or pipeline, who should be responsible for the interception or destruction of this device? Resolving this issue is fundamental for the acquisition of technical equipment such as anti-drone systems.

Furthermore, unmanned platforms can support the protection of shipping and infrastructure, especially in a surveillance function. In this respect, another matter that should be regulated is whether, for example, underwater pipeline or cables should be monitored by drones operated by the Navy, the Border Guard or the infrastructure owner. Poland recently decided to upgrade Hugin underwater drones for pipeline surveillance.[33] However, as they are part of the mine countermeasure force and also have other tasks, this may only be an interim solution and greater efforts may be required.

3.6 International cooperation

Given the current geopolitical situation and the fact that most of the states bordering the Baltic Sea are now members of NATO and the EU, intensifying international cooperation is a logical conclusion.

Most prominently, the recent implementation of NATO's multi-domain vigilance activity Baltic Sentry aims at enhancing allied maritime situational awareness. In addition, the development of Task Force X aims to add a sufficient uncrewed component to allied enhanced vigilance activities. The Baltic states are already involved in multiple programmes, for example cross-Baltic pipelines (Baltic Pipe, Baltic Connector). Also, since not only these states are threatened by Russia's hostile actions, the implementation of an agreement such as the North Sea security agreement signed by Belgium, Denmark, Germany, the Netherlands, Norway and the United Kingdom in 2024[34], which facilitates a better exchange of information and a coordinated response to identified threats, is vital. In addition, international cooperation could allow for sharing the costs of building and maintaining sensor networks, thus enabling a better monitoring of Russian maritime activities. It could also enable the joint acquisition of maritime surveillance platforms such as maritime patrol aircraft (MPA) and ships. As regards patrol aircraft, it should be noted that while Germany has purchased eight P-8 Poseidon aircraft and five such planes were delivered to Norway, most of the Baltic Sea countries have only limited or no surveillance capabilities. Denmark operates four Cl-604 jets that can be used in a maritime patrol role apart from their transport mission; similarly, Finland has three

32 For further information, see Łukasiewicz et al. 2021.
33 Zalesiński 2023.
34 Chiappa 2024.

Learjet 35 planes that can be used as MPAs. Poland does have a designated patrol squadron equipped with M-28 Bryza light patrol planes.

Apart from the P-8s, however, all those platforms lack anti-submarine warfare capabilities. They are supplemented by border guard planes and helicopters, but law enforcement airplanes also do not have ASW equipment.

As regards helicopters, only Germany, Denmark, Sweden, Norway and Poland have ASW-capable machines, and in most of those states, they are also tasked with missions outside the Baltic Sea (especially deployments on board of warships). In the case of Poland, older helicopter types (Mi-14PŁ and SH-2G Seasprite) will soon be decommissioned, and so far, only four AW101 helicopters have been contracted – a number that is much smaller than necessary to cover all requirements[35].

Also, maritime patrol aircraft are costly – joint procurement could allow for multiple countries to benefit from their capabilities, in a manner similar to existing programmes such as NATO's multinational AWACS force[36] or its tanker/transport fleet (MRTT-C)[37].

When it comes to ships, there are generally no multinational fleets. However, it is possible to have several ships of the same class built together, especially if several countries have similar requirements – as in the case of the type 212CD submarines (a joint German-Norwegian purchase) or the older Tripartite-class mine warfare ships. There are obstacles, certainly: different requirements, different budgets and political factors shaping procurement decisions. However, several possible options can be pointed out. For example, the Swedish parliamentary defence commission suggested building four more corvettes, supplementing the already procured Luleå-class vessels[38]. If Sweden decided to purchase additional corvettes, that would pave the way for a possible cooperation with Poland to also acquire four corvettes, provided the Moray programme is implemented as announced.

Another field of cooperation in the Baltic region could be mine-countermeasures forces. Several countries have ships built more than twenty-five years ago, including Germany (Frankenthal class) and Sweden (Koster class), and sooner or later those vessels will need replacement. The smaller Baltic states, Lithuania, Latvia and Estonia, all operate older mine warfare ships that they received from Western Europe. The replacement of those vessels might also be part of a joint programme.

Also, submarine programmes are another potential area of cooperation, especially in the case of Poland.

4 Summary

The Russo-Ukraine war casts a shadow on the perception of contemporary threats, and the maritime domain is no exception. From a Polish perspective, the main lesson is that there are no direct lessons. There are different environmental, political and military conditions to consider.

On the one hand, the Russian armed forces have performed differently than expected in many areas. On the other hand, hybrid attacks, especially those targeting maritime

35 IISS, The Military Balance 2024.
36 NATO 2024a.
37 NATO 2022.
38 Häggblom 2024.

critical infrastructure, represent major risks compared to open, conventional attacks as seen in the invasion of Ukraine. Hybrid attacks may bring significant damage to the affected country's national economy and social stability, and a failure on our part to protect this infrastructure and the services provided by it may allow for more successful Russian hybrid operations in the future. This risk is enhanced by the growing importance of the Baltic Sea to Poland despite the existing sea blindness.

Therefore, among the listed recommendations, tackling sea blindness must be considered fundamental, followed by the formulation of a national maritime strategy. Without those steps, any further ones cannot be planned predictably. A planned development approach, however, is particularly important for shipbuilding.

From a Polish perspective, due to the long-standing neglect of its naval forces, the continuation of already started programmes and the planned, systematic development of its future fleet are of crucial importance in order to be able to assume a significant role in Baltic Sea security.

Bibliography

8th FOW (2024): Niszczyciele min typu Kormoran II (proj. 258), https://www.wojsko-polskie.pl/8fow/kormoranii/, last accessed on: 28-09-2024.

Act of Parliament of the Republic of Poland on State Border Protection, 1991 (with amendments).

Act of Parliament of the Republic of Poland on the Border Guard, 1990 (with amendments).

Associated Press (2023): Poland Detains 9 People Suspected of Spying for Russia, in: Associated Press dated 16-03-2023, https://apnews.com/article/espionage-poland-ukraine-russia-belarus-sabotage-foiled-a105984d15ddc200369d8b13ca37f4b6, last accessed on: 14-09-2024.

Associated Press (2024): Baltic Sea Nations React Warily to a Reported Russian Proposal to Revise Its Maritime Border, in: Associated Press dated 23-05-2024, https://apnews.com/article/baltic-sea-russia-security-border-fb9849dd556fa166f1135172c6935c9d, last accessed on: 14-09-2024.

Braw, Elizabeth (2024): Russia's Growing Dark Fleet: Risks for the Global Maritime Order, in: Atlantic Council dated 11-01-2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-growing-dark-fleet-risks-for-the-global-maritime-order/, last accessed on: 21-12-2024.

Chiappa, Claudia (2024): 6 Countries Move to Protect the North Sea from Russians, in: Politico dated 09-04-2024, https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/, last accessed on: 21-12-2024.

Ciślak, Jarosław (2024a): Czy powstanie nowy Hydrograf? [ANALIZA], in: Defence24 dated 17-09-2024, https://defence24.pl/sily-zbrojne/czy-powstanie-nowy-hydrograf-analiza, last accessed on: 22-12-2024.

Ciślak, Jarosław (2024b): MON zadeklarował realizację programów Ratownik, Orka i dozbrojenie Ślązaka, in: Defence24 dated 28-11-2024, https://defence24.pl/sily-zbrojne/mon-zadeklarowal-realizacje-programow-ratownik-orka-i-dozbrojenie-slazaka, last accessed on: 22-12-2024.

Dalsjö, Robert/Berglund, Christofer/Jonsson, Michael (2019): Bursting the Bubble? Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications, in: FOI dated March 2019, https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4651--SE, last accessed on: 23-09-2024.

Eggert, Konstantin (2024): GPS Jamming in the Baltic Region: Is Russia Responsible?, in: Deutsche Welle dated 05-05-2024, https://www.dw.com/en/gps-jamming-in-the-baltic-region-is-russia-responsible/a-68993942, last accessed on: 14-09-2024.

Polityka energetyczna Polski do 2040 r (*Energy Policy of Poland until 2040*), https://www.gov.pl/web/klimat/polityka-energetyczna-polski, last accessed on: 24-09-2024.

Frederick Bryan/Charap Samuel/Mueller Karl P (2022): Responding to a Limited Russian Attack on NATO During the Ukraine War, in: RAND dated 20-12-2022, https://www.rand.org/pubs/perspectives/PEA2081-1.html, last accessed on: 29-09-2024.

GUS (2024): Gospodarka morska w Polsce w 2023 roku, in: Główny Urząd Statystyczny dated 29-04-2024, https://stat.gov.pl/obszary-tematyczne/transport-i-lacznosc/transport/gospodarka-morska-w-polsce-w-2023-roku,7,21.html, last accessed on: 27-09-2024.

Häggblom, Robin (2024): Sweden Looking at More Surface Combatants and Submarines, in: Naval News dated 29-04-2024, https://www.navalnews.com/naval-news/2024/04/sweden-looking-at-more-surface-combatants-and-submarines/, last accessed on: 29-09-2024.

Hartog, Eva (2024): Russia Mysteriously Deletes Threat to Redraw Baltic Sea Border, in: Politico dated 22-05-2024, https://www.politico.eu/article/russia-defense-ministry-change-baltic-sea-border-finland-latvia/, last accessed on: 14-09-2024.

IISS (2024): The Military Balance 2024, Routledge: Abingdon-on-Thames, UK.

Kamiński, Rafał (2024a): Marynarka Wojenna chętna także na korwety? Wielki powrót programu "Murena", in: Gospodarka Morska dated 09-05-2024, https://www.gospodarkamorska.pl/marynarka-wojenna-chetna-takze-na-korwety-wielki-powrot-programu-murena-77936, last accessed on: 27-09-2024.

Kamiński, Rafał (2024b): Do trzech razy sztuka? Agencja Uzbrojenia zamówi okręt ratowniczy programu "Ratownik", in: Gospodarka Morska dated 15-11-2024, https://www.gospodarkamorska.pl/do-trzech-razy-sztuka-agencja-uzbrojenia-zamowi-okret-ratowniczy-programu-ratownik-81685, last accessed on: 22-12-2024.

Kaushal, Sidharth (2023): Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure, in: RUSI Commentary dated 25-05-2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure, last accessed on: 28-09-2024.

Lange Heinrich/Combes, Bill/Jermalavičius, Tomas/ Lawrence, Tony (2019): To the Seas Again. Maritime Defence and Deterrence in the Baltic Region, in: International Centre for Defence and Security dated 16-04-2019, https://icds.ee/wp-content/uploads/2019/04/ICDS_Report_To_the_Seas_Again_Lange_Combes_Jermalavicius_Lawrence_April_2019.pdf, last accessed on: 24-09-2024.

Łukasiewicz Jędrzej/Piekarski Michał/Kluczyński Maciej (2021): Security of Infrastructure Critical to Threats from Unmanned Platforms, The Raport PTBN, Volume II, https://drive.google.com/file/d/1hCHNae2847TwpHQjE-KcBwAI4SreDt4Y/view, last accessed on: 29-09-2024.

Marszałkowski, Mariusz (2023): Rosjanie szpiegują na Bałtyku? Podejrzana aktywność u morskich granic Polski, in: Biznes Alert dated 23-01-2023, https://biznesalert.pl/polska-baltyk-statki-wywiad-rosja-bzpieczenstwo-gdansk-naftoport/, last accessed on: 27-09-2024.

Meurmishvili, Ia (2017): Russian Mystery Weapon Claim Seen as Sign of Military

Weakness, in: Voice of America dated 02-05-2017, https://www.voanews.com/a/russian-mystry-weapon-claim-seen-as-sign-of-military-weakness/3834792.html, last accessed on: 26-09-2024.

Murphy Martin/Hoffman Frank G./Schaub jr Gary (2016): Hybrid Maritime Warfare and the Baltic Sea Region, in: Centre for Military Studies, University of Copenhagen dated November 2016, https://cms.polsci.ku.dk/publikationer/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf, last accessed on: 29-09-2024.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (*National Security Strategy of Republic Of Poland*) (2020): https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, last accessed on: 24-01-2025.

NATO (2022): Multi Role Tanker Transport Capability (MRTT-C), https://www.nato.int/nato_static_fl2014/assets/pdf/2022/9/pdf/2209-factsheet-mrtt.pdf, last accessed on: 30-09-2024.

NATO (2024a): E-3A Component 2024, https://awacs.nato.int/page5835237, last accessed on: 24-01-2025.

NATO (2024b): Washington Summit Declaration, dated 10-06-2024, last updated 15-06-2024, https://www.nato.int/cps/en/natohq/official_texts_227678.htm, last accessed on: 30-09-2024.

Navy Lookout (2023): A Guide to RFA Proteus – the UK's New Seabed Warfare Vessel, in: Navy Lookout dated 10-10-2023, https://www.navylookout.com/a-guide-to-rfa-proteus-the-uks-new-seabed-warfare-vessel/, last accessed on: 22-12-2024.

PGZSW (2024): Miecznik – wielozadaniowe fregaty dla MW RP, https://pgzsw.com.pl/oferta/program_miecznik/, last accessed on: 26-09-2024.

Port Gdańsk (2024): Facts and Figures, https://www.portgdansk.pl/en/business/general-information/facts-and-figures/, last accessed on: 26-09-2024.

Ptak, Alicja (2024): Poland Charges Nine People Suspected of Sabotage on Behalf of Russia, in: Notes from Poland dated 21-05-2024, https://notesfrompoland.com/2024/05/21/poland-charges-nine-people-suspected-of-sabotage-on-behalf-of-russia/, last accessed on: 14-09-2024.

Rubin (2024): Rubin Robotics, https://ckb-rubin.ru/en/projects/robototekhnika/, last accessed on: 27-09-2024.

Sutton, H I (2022): Russian Underwater Drone with Manipulator Arm for Seabed Operations, in: Covert Shores dated 29-09-2022, http://www.hisutton.com/Russian-Intervention-Underwater-Drone.html, last accessed on: 27-09-2024.

Sutton, H I (2024): Overview of Maritime Drones (USVs) of the Russo-Ukrainian War, 2022-24, in: Covert Shores dated 21-09-2024, http://www.hisutton.com/Russia-Ukraine-USVs-2024.html, last accessed on: 27-09-2024.

Trade.gov.pl (2024): Polskie porty morskie w 2024 roku, in: Trade.gov.pl dated 16-01-2025, https://www.trade.gov.pl/aktualnosci/polskie-porty-morskie-w-2024-roku/, last accessed on: 23-01-2025.

Wiese Bockmann, Michelle (2024): Finland police seize Russian-linked dark fleet tanker Eagle S in cable-cutting investigation dated 26-12-2024, https://www.lloydslist.com/LL1151950/Finland-police-seize-Russian-linked-dark-fleet-tanker-Eagle-S-in-cable-cutting-investigation, last accessed on: 15-03-2025.

Wilewski, Krzysztof (2023): Poznaliśmy uzbrojenie Mieczników, in: Polska Zbrojna dated 15-12-2023, https://polska-zbrojna.pl/home/articleshow/40881?t=Poznalismy-uzbrojenie-Miecznikow, last accessed on: 26-09-2024.

Wojsko Polskie (2024): Wodowanie i chrzest przyszłego ORP Jaskółka,

https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2024-06-27v-wodowanie-i-chrzest-przyszego-orp-jaskoka/, last accessed on: 27-09-2024.

Zalesiński, Łukasz (2023): Dron sprawdzi rurociągi, in: Polska Zbrojna dated 10-11-2023, https://www.polska-zbrojna.pl/home/articleshow/40660?t=Dron-sprawdzi-rurociagi, last accessed on: 30-09-2024.