

WAR IN UKRAINE. ANALYSIS SECURITY OF MARITIME CRITICAL INFRASTRUCTURE IN THE BLACK SEA REGION

O.V. Akimova

Keywords: maritime transportation system, maritime critical infrastructure, security assessment, war in Ukraine.

Abstract.

The Black Sea is an area of significant geostrategic importance, bridging Europe to Asia, with untapped potential for economic development, strategic transit routes especially for access to energy resources and critical raw materials.

Its critical importance is underscored by Russia's war of aggression against Ukraine that has shaken the foundations of the rules-based international order and exposed the vulnerabilities of European and regional security. It has plunged regional security to its lowest point since the past two decades involve numerous crises of varied origins and nature. This indicates the shrinkage of forecasting horizon or even total lack of forecasting capability in the contemporary security management mechanisms, their inability to prevent low-probability emergencies of sophisticated nature, such as US terrorist attacks of 9/11, Hurricane Katrina in the US (2005), world financial crisis (2008), destructive earthquake and tsunami causing a Fukushima Daiichi Nuclear Power Plant accident in Japan (2011), events of the Arab Spring (2011), refugee crisis in the EU? War in Ukraine. Analysis of these, as well as the other large-scale and comprehensive challenges to regional and global security, as well as lessons learned from them and calls for a robust, coordinated EU response assure protection of objects, systems and resources critical for the existence of the state (the critical infrastructure) against all types of threats and their combinations. In this evolving geopolitical landscape, with the Black Sea region at its core, the EU is stepping up with a comprehensive approach with the aim of supporting the democratic resilience of a region vital to Europe's stability and prosperity and asserting our interests.

INTRODUCTION

Protection of critical infrastructure as a security target emerged during the Cold War and became an actively developing trend in the leading countries in the beginning of this century in response to abrupt growth of a terrorist threat. This security area is seen as a priority by such international structures as the EU and NATO since, in addition to obvious benefits and advantages, globalization and IT development increase economic, financial, technological and resource interfaces

and interdependences between different countries and their alliances, as well as between world regions, making modern society highly vulnerable to threats – in particular those targeting the nodal points of the described interfaces.

Realization of the growing terrorist threats in Europe caused the European Commission to develop and, in November 2005, publish the Green Paper on the European Programme for Critical Infrastructure Protection [1], and subsequently, in 2006, on completion of the consultations between the EU countries, the European Programme for Critical Infrastructure Protection [2]. Character of the EU approach specific for a community of independent states was reflected in the EC document entitled Protecting Europe's Critical Energy and Transport Infrastructure (February 2007) [3] and in a special directive for the identification of critical infrastructure objects and assessment of a need to enhance their protection (December 2008) [4]. Protection of critical power supply infrastructure was named a priority focus for the assurance of energy security of NATO member states and the Alliance in general in the Declaration of the Chicago Summit (20 May 2012).

The Ukrainian state currently faces the most serious security challenge in its entire independence period. Acute social and political crisis against the backdrop of foreign military involvement in the internal affairs of Ukraine, abrupt surge of extremism and terrorism, unseen growth of crime, including armed, decline of economy and expanding humanitarian crisis in the eastern regions of the country, destruction or damage of numerous enterprises and infrastructure objects are the factors that define the new reality in which Ukraine currently exists and in which security of its citizens, the society and state institutions should be assured.

Quite obviously, the Ukrainian security sector is under a radical reform that should use international experience cause the declared course toward integration in the EU. In the current environment, the factors described above make implementation of the critical infrastructure concept, actively used in leading Western countries, the EU and NATO member states as one of the security policy tools, particularly topical. [4]

The EU is committed to supporting Ukraine and its neighbours, by upholding their independence, sovereignty and territorial integrity, fostering peace and dialogue, providing security guarantees and contributing to recovery and reconstruction. The security in the Black Sea region will equally need to be at the heart of a just, comprehensive and lasting peace [5].

THE RESEARCH PROBLEM IDENTIFICATION

Although each actor, from individual to country even to international organizations [6, 7], has a subjective definition of critical infrastructure, the fact that they cannot be dispensed with, let alone that their inadequacy would cause serious problems, is the common content of the definitions of

critical infrastructure. Critical infrastructure (CI), which consists of systems that perform important functions of a country or region and affect the life of a community, covers almost every area, from a city's water network to the huge underwater communication cables that pass through the Pacific. Although CI operating in such a comprehensive framework, in all areas of life and interdependently, has a different sector for each country, generally accepted CI sectors are listed in figure 1. Each CI sector is considered highly important in terms of its field of activity and the sectors it affects.



Figure 1: Critical Infrastructure Sectors (Resource: <https://www.marseccoe.org/wp-content/uploads/2023/10/Maritime-Critical-Infrastructure-Protection-.pdf>)

However, these include lifeline sectors usually defined as sectors that ensure the continued operation of critical business and government functions and provide vital services that, if compromised or not promptly reinstated, may put human health and safety or national and economic security at risk. These industries offer products and services that are essentially ubiquitous but can create life-threatening conditions in the event of a short-term absence. While the four lifeline sectors may vary for each country or region, it is seen that especially the **energy, water, transportation and communication** sectors are common to many actors.

As mentioned before, each actor has a definition of CI within the scope of its own priorities and agendas. However, specifically addressing the CI definitions of several important actors, and NATO's especially, is important.

“Within NATO, Critical Infrastructure is a general term describing a nation's infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political, and/or social life on which a nation and/or NATO depends and from an Allied Command Operations (ACO) perspective, critical infrastructure is categorized into three different sub-categories Critical National Infrastructure (CNI), Mission-Vital Infrastructure (MVI) and Key Infrastructure (KI).”

According to this definition, it is seen that NATO considers the concept of CI from the perspective of allied countries on the one hand, on the other hand, it carefully focuses on CI that may

create a disadvantage for the operational power of the Alliance. Two key NATO documents published in 2022 also show traces of strategies for critical infrastructure: in the NATO 2022 Strategic Concept: “We will pursue a more robust, integrated, and coherent approach to building national and Alliance-wide resilience against military and non-military threats and challenges to our security, as a national responsibility and a collective commitment rooted in Article 3 of the North Atlantic Treaty.

We will work towards identifying and mitigating strategic vulnerabilities and dependencies, including with respect to our critical infrastructure, supply chains, and health systems.”

Similarly, the NATO 2030 document emphasizes that, in line with the CNI sub-category, necessary support would be provided for the protection of CI upon the request of the allied countries in order to increase the resilience of the alliance [8. 9].

Besides NATO, the EU defines CI as:

“a system or part thereof located in the 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” [10].

Referring to the experience of leading nations in development of approaches to assuring national security through application of the critical infrastructure concept the following definition of this term for Ukraine:

“critical infrastructure of Ukraine shall mean and include systems and resources, whether physical or virtual, that support functions and services whose disruption will cause most severe negative effects for activity of the society, socioeconomic development of the country and national security” [11].

According to EU Council Directive 2008, in order for the damage to the CI of an EU member state to be considered within the scope of "European Critical Infrastructure (ECI)", the deterioration of the relevant CI must affect at least two member states: The International Criminal Police Organization (INTERPOL) uses an effective definition of “Critical infrastructure as the life support system of our everyday existence” and for critical infrastructure, they emphasize that the monitoring/control facilities created by the merger of the digital and physical worlds also pose a significant security vulnerability. For this reason, the awareness of vulnerabilities in sectors of critical infrastructure, particularly in light of the rising new generation threats of the current century, has prompted states to take a proactive approach towards protecting themselves.

As for the spectrum of critical infrastructure threats existing in Ukraine, their nature is shaped by the security environment currently faced by the country. Hostilities as part of the Anti-Terrorist Operation in Donbas Region, featuring high level of wear of capital assets and serious problems with environmental and anthropogenic safety, rapidly increases the level of threat of accidents at high

hazard assets such as coal mines, power sector facilities, chemical factories and steelworks, as well as in the utility networks, whether as the result of incidental damage or loss of process control or as a consequence of terrorist acts or sabotage.

No doubt, developments in the Eastern Ukraine will have significant impact on threats to the national critical infrastructure. In particular, it should be expected that a high level of terrorist, sabotage and criminal threats to critical infrastructure is likely to persist in a long run as the result of today's crisis.

The existing Ukrainian legal framework governing issues allied to critical infrastructure protection classifies emergencies, rather than threats, *inter alia* based on their origin. Article 5 of the Civil Protection Code of Ukraine specifies that, depending on origin of events that may cause emergency situations in Ukraine, the following types of emergency situations could be distinguished:

1) man-induced; 2) natural; 3) social; 4) military.

In our view, this classification cannot be adopted straightforwardly for the classification of critical infrastructure threats since it has some methodology reservations and blocks some of the advantages offered by implementation of the critical infrastructure protection concept.

It makes more sense to define the following classes of threats for the purposes of critical infrastructure protection in Ukraine:

accidents and technical failures, including air crashes, nuclear accidents, fires, power supply system accidents, releases of hazardous substances etc., system failures, accidents and emergencies caused by negligence, administrative errors etc.;

hazardous natural phenomena, including extreme weather conditions, forest, steppe and peat-bog fires, seismic events, epidemics and pandemics, cosmic phenomena, hurricanes, tornadoes, earthquakes, tsunamis, floods, etc.;

malicious acts, including malicious acts of groups or individuals, such as terrorists or criminals, as well as hostilities under conditions of war.

The highest is the hazard from combined threats and threats whose materialization may cause disastrous and varied cascade effects as the result of interdependence of critical infrastructure elements.

The Ukrainian legislation concerning protection of assets that, based on the international practice, are attributed to critical infrastructure, is rather diverse and includes numerous regulations, mostly at the departmental scale.

Applicable legislation provides for the following categories of assets subject to special protection and operation regimes:

enterprises of strategic significance for economy and national security [11];

vital assets in energy sector [12];

vital assets in oil and gas sector [13];
important governmental facilities, including control centers of government agencies and local government bodies [14];
potential terrorist targets [15];
assets to be protected and defended in emergency and during special periods[16]; assets subject to mandatory protection by State Protection Service on a contractual basis [17];
high hazard facilities [18] (including from the List of Extremely Hazardous Enterprises Whose Operation Requires Special Arrangements for the Prevention of Detriment to Human Life and Health and to Property, Installations, and the Environment [19]);
assets included in the State Register of Potentially Hazardous Facilities [21]; radiological hazard facilities subject to development of a facility-level design basis threat (DBT) [22];
assets assigned civil protection categories [23].

ANALYSIS SECURITY OF MARITIME CRITICAL INFRASTRUCTURE (MCI) IN THE BLACK SEA REGION

Maritime critical infrastructure (MCI) is part of a country's national critical infrastructure. Maritime critical infrastructure protection (MCIP) refers to measures taken to ensure the security and resilience of maritime infrastructure essential to the functioning of a country or region. These measures include such as safeguarding ports, shipping routes, chokepoints, offshore energy installations, Seelines of Communication (SLOC) etc. along with ensuring the security of the information and communication infrastructures that underpin these operations. MCI constitutes one of the cornerstones of maritime security because it plays a critical role in ensuring the safety and security of maritime operations, and MCIP is held in a special position in the security strategies of countries since threats in the sea area are more difficult to prevent than threats on land. Especially in the post-Cold War period, the multidimensional transformation of security and the emergence of new threat perceptions have necessitated the multidimensional consideration of maritime security. Although analytically, there are three dimensions to maritime security: inter-state, maritime terrorism, and blue crime, the complex nature of maritime security threats blurs the line between these distinctions and requires a different perspective on maritime security. The concept of maritime security has attracted attention in security studies after the 1990s in parallel with the changing nature of international relations, and just like the concept of security itself, it does not have a common definition. But, if there is a common judgment for maritime security, it is that maritime security is not a given. In other words, it is not possible to talk about maritime security in the natural situation and it is essential for states to monitor the maritime area for constructing and ideally achieving Maritime

Situational Awareness (MSA) so that they can utilize that awareness in pointing out and addressing potential threats or critical vulnerabilities in order to ensure maritime security. Maritime security is also a framework concept because of the sub-themes it contains. In this direction, maritime security has an inclusive quality that covers the fight against all threats arising from state or non-state actors through maritime areas by including many concepts which are defined as threats to lifeline CI in the maritime environment such as energy security, maritime terrorism, climate change, etc. (Figure 2):

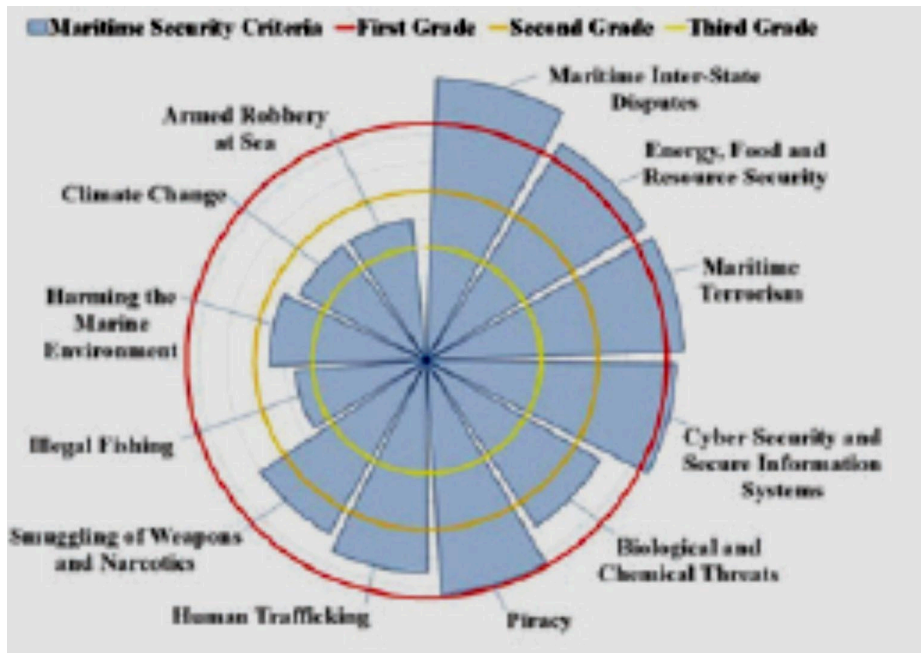


Figure 2: Threats to Lifeline Critical Infrastructure in the Maritime Environment

[Resource: Oktay Çetin and Mesut Köseoğlu, 'A Study on the Classification of Maritime Security Threat Topics', International Journal of Environment and Geoinformatics 7, no. 3 (6 December 2020): 369, <https://doi.org/10.30897/ijegeo.742336>].

Along with the awareness of maritime security, the increase in academic studies and the taking of important steps by international actors on maritime security have gained momentum, especially in the current century. The main reason for this situation is that the incidents of maritime terrorism, which increased in the 2020s, reinforced the collective awareness of maritime areas. At the same time, the oceans, which have served humanity for millennia and provided food and livelihoods to three billion people, have gained more importance, especially with technological developments and globalization [23].

The maritime transport infrastructure supports the maritime transport system and is the physical base to provide all the necessary services for the system functions. It consists of ports with their intermodal connections, seaways, ships and management systems. The security of the physical and the informational maritime transport infrastructures is fundamental for the system functions [24].

Major Black Sea ports include Odessa (Ukraine), Constanța (Romania), Varna & Burgas (Bulgaria), Novorossiysk & Tuapse (Russia), and Batumi (Georgia), handling diverse cargo like grain, oil, and containers, though recent geopolitical conflicts have significantly impacted Ukrainian ports like Odessa and Chornomorsk, affecting global trade routes. These strategic ports facilitate crucial trade for bordering nations and connect to international shipping lanes, with key players specializing in different goods, such as petroleum (Novorossiysk, Batumi) or general cargo (Odessa, Constanța), figure 3.

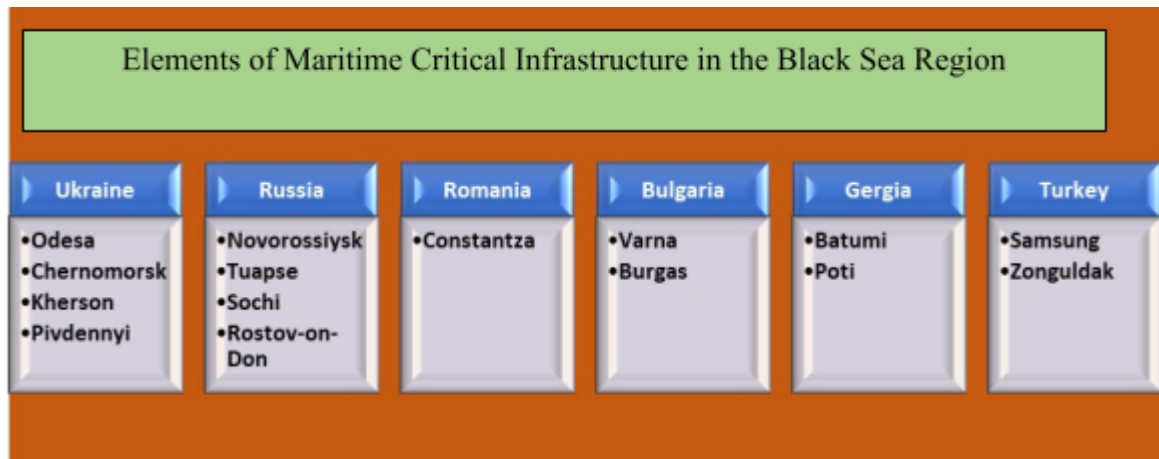


Figure 3. Elements of Maritime critical infrastructure in the Black Region

Resource: Autor

Russia's war of aggression has a significant negative impact on trade dynamics in the Black Sea region and globally. The disruption of Ukrainian grain exports initially has contributed to rising global food prices and global food insecurity. In response, the EU-Ukraine Solidarity Lanes [25] established new transport routes, providing a lifeline to the Ukrainian economy. Even more important, the Solidarity Lanes continue providing vital new transport routes, including for non-agricultural Ukrainian export to the EU as well as for EU exports to Ukraine. The total value of trade via the Solidarity Lanes since May 2022 is around EUR 213 billion, including around EUR 150 billion imports to Ukraine. Over EUR 2 billion has been mobilised to scale up the Solidarity Lanes, including contributions by the Commission, the European Investment Bank, the European Bank for Reconstruction and Development, and the World Bank [26]. Ukraine's successful establishment of a new maritime corridor has helped restore exports of grain from its Black Sea ports, a development further supported by the sustained capacity offered by Ukrainian Danube ports that link directly to Black Sea or EU seaports.

Despite these successful efforts, Russia's regular and targeted attacks continue to impede transport and overall investment in regional projects and infrastructure and lead to high insurance

costs. Substantial investments will be needed not only to reconstruct the transport infrastructure in the Black Sea and Danube region, which has suffered extensive damage due to repeated attacks, negatively impacting trade, raising costs and undermining reliability of transport, but also to upgrade and modernise the outdated infrastructure, logistics systems and border control equipment to meet EU standards.

As a direct response to the adverse consequences on trade dynamics in the Black Sea region and globally caused by Russia's war of aggression, the Trans-Caspian Transport Corridor (TCTC) has seen trade volumes doubling in 2022, with a surge in demand leading to significant increase in container traffic. Effectively tackling bottlenecks and capacity shortages would create an economically viable alternative for private sector operators seeking to diversify trade routes, as well as shrinking the current estimated transit time of 14-45 days [27].

Maritime physical Security Threats

Physical threats to maritime security can originate from the air, land or sea and are generally easier to identify compared to virtual threats. These threats can include, figure 4:



Figure 4. Maritime physical Security Threats

Resource: Author

Physical attacks: ships may come under attack from various weapons launched from aircraft (including helicopters, ships, submarines and land-based sites. These weapons have included bombs, rockets, machine guns. Water-Borne Improvised Explosive Devices (WBIEDs) one way attack drones and missiles. In addition to one way attack drones. Unmanned Aerial Vehicles (UAVs) and Uncrewed Surface Vehicles (USVs) may also be used for surveillance and to support loitering munitions in conducting attacks [28].

actors.

Seizure: ships have been illegally seized and held for prolonged periods by state and non-state

Piracy: pirates use various boat configurations, including small

high-speed skiffs and motherships, which allow them to operate over larger areas. They typically use small arms and Rocket Propelled Grenades (RPGs) to intimidate shipmasters and attempt to board the ship using ladders or ropes. Successful boardings are more likely at night.

Illegal boardings: in addition to piracy boardings using ladders and hooks, more aggressive boardings have been seen involving fast attack boats and helicopters to land or fast-rope forces onto a deck.

Criminal activity: illegal boarding with intent to steal shipboard equipment or seafarers' possessions, money, etc., is commonplace in some ports. Such attackers can be armed, most usually with bladed weapons, and can present a physical threat to crews. Such threats usually, but not exclusively, occur in traffic separation schemes where dense traffic exists, and territorial waters, particularly ports and anchorages. Illegal boardings may also occur while a ship is underway. In many cases, the intent is to steal, rather than taking control of the ship.

Specific Threats

Water Borne Improvised Explosive Devices (WBIEDs): These have been used against merchant ships in conflict regions. WBIEDs can be crewed or uncrewed surface vessels. Incidents have occurred where a WBIED has been controlled from a distance or from an accompanying mothership or operates autonomously. Mitigation measures to prevent contact with the ship's hull are limited. Masters should recognise the intent of these attacks is to cause damage and not necessarily to board the ship.

Sea mines: a sea mine is an explosive device laid in the water with the intention of damaging or sinking ships or of deterring shipping from entering an area. The term does not include devices attached to the bottom of ships or to harbour installations by personnel operating underwater, nor devices which explode immediately on expiration of a predetermined time after laying. Mines are designed to deny access to ports

and sea lanes and can be classified as moored, bottom, or moving mines.

a. Moored mines (also known as buoyant mines): a mine of positive buoyancy held below the surface by a mooring attached to a sinker on the seabed. Its firing system can be of either contact or influence type. Some 'deep moored mines' use extremely strong moorings (usually small



gauge wire) 10 permit use in water depth down to 1,000 metres. If the mooring cable breaks, then the moored mine becomes a moving (floating) mine.

b. Bottom/ground mines: bottom/ground mines are negatively buoyant devices that rest on, or can become buried in, the seabed and are held there by their own mass. The firing system is usually of the influence type. They can be triggered by any influence (acoustic, magnetic, seismic, pressure), or a combination of these influences. These types can be laid up to maximum water depths of 120m, depending on the target and/or the amount of explosive charge, but water depths up to 60m are more suitable.

c. Moving mines: this is a collective description of mine types that are not stationary. All floating, oscillating, rising or homing mines belong to this category. As an example, rising mines can be laid at a depth of 5(X)m (mine case) and 2.400m (anchor)

d. Limpet mines: these are commonly manually attached by a swimmer or diver on the underside of a ship's hull, usually with magnets. Unlike larger mines, limpet mines are not intended to sink a ship but immobilise it.

If there is intelligence suggesting the presence of sea mines in an area, visual sightings, or a confirmed explosion from a sea mine, then a Mine Threat Area (MTA) or a Mine Danger Area (MDA) would be established and broadcast to maritime traffic via navigational area (NAVAREA) Warnings.

Anti-Ship Missiles.

Anti-Ship Missiles (ASM) are long range, accurate and powerful weapons and have been used against merchant ships in the Red Sea. Other ships may be hit if the missile controller targets the wrong ship or the missile homes in on an unintended target. They pose a significant threat due to their destructive power causing fatalities and catastrophic damage.



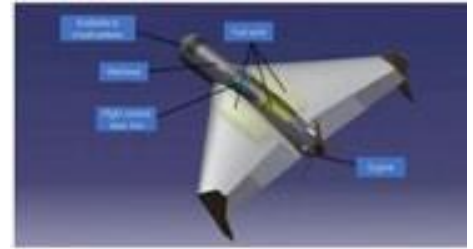
ASMs can be launched from a variety of ships, submarines and aircraft as well as from land. They can be launched from short range to hundreds of miles. These missiles can be of a cruise or ballistic nature:

Cruise missiles are jet-propelled and travel at subsonic speeds. Their sensors are very accurate. Ballistic missiles are rocket-powered to get into flight, after which they follow an arching trajectory to the target. The launch of an ASM may be detected through a visible flash and smoke. Missiles will normally hit above the waterline. The main hazard is likely to come from fire, caused either by the warhead explosion or by the unspent fuel from the missile motor.

Missiles can be fired in a straight line or follow a predetermined course to a target or dead reckoning (DR) position. They can have an active or passive seeker head using optical, electronic or heat signature homing to locate targets.

Loitering Munitions.

Loitering Munitions (LM) are a form of UAV with a built-in weapon and the capability to loiter (wait passively) in the target area until the target is located. The number of LM attacks against both civilian and military ships, especially in the Red Sea and Middle East, has risen. The global proliferation of these rapidly advancing autonomous technologies, to both state and private actors, poses a significant security threat to commercial shipping.



Virtual security threats.

Virtual threats primary involves cyber-attacks on electronic systems, which can impact ship navigational systems, disrupt Global Navigation Satellite System (GNSS) or spoof Automatic Identification System (AIS) services. These threats are harder to detect and require comprehensive procedures such as:

- Backup systems and processes.
- Situational awareness training.

Regional maritime threats.

Maritime security threats vary globally and within geographical regions. A variety of threats may be present in any one area at varying intensities depending on the intent and capability of attackers. Recognising this, reporting centres and industry associations produce information on regional threat actors, their intent and capability to attack merchant shipping, and link these to applicable BMP measures to mitigate the threat.

To mitigate these threats, continuous improvement through regular security drills and exercises, capturing lessons observed, and adapting to new technologies is essential. Merchant ships should maintain close coordination with military forces and leverage commercial intelligence and open-source services for threat updates.

War in Ukraine – impact on maritime situation in the Black Sea Region

Despite ongoing peace talks between Ukraine and Russia, the security situation in the Black Sea remains unstable. All port calls in the region should be assessed on a case-by-case basis, consulting best management practices for guidance on threats and mitigating measures.

The shipping association's Maritime Industry Security Threat Overview (MISTO), last updated on 26 November 2025, emphasises that both Ukraine and Russia have the capability and opportunity to strike ships and port facilities within the Black Sea region. Regarding intent, Russia has declared that all merchant ships heading for Ukrainian Black Sea ports are considered legitimate military targets, while Ukraine has made the same claim for merchant ships bound for Russian Black

Sea ports. Although direct attacks on merchant ships at operating in the Black Sea have so far been limited, both sides have increasingly used drones to target ports, energy infrastructure, and in recent weeks, ships underway. This raises concerns about a possible shift in the threat to commercial shipping and an elevated risk of collateral or unintended damage.

According to the Romanian Military Ministry of National Defence, a stray mine posing a hazard to navigation was detected and neutralised by the Romanian Naval Forces as on 3 December 2025, approximately 36 nautical miles east of Constanza. The Ministry further reports that over the past four years, around 150 sea mines have been neutralised in the Black Sea, including seven by Romanian Naval Forces.

Drifting mines, along with drones used by both sides to strike ships and shore infrastructure, underscores the ongoing threat to maritime operations in the Black Sea into 2026.

Key considerations before approaching the Black Sea Ships in transit.

According to the NATO Shipping Centre (NSC), the threat of collateral damage or direct hits on civilian shipping within the war risk area (NAVAREA III warning 0124/2022) in the northern part of the Black Sea, west of Crimea, remains high.

Following a series of drone strikes against ships and port infrastructure in the Black Sea in late 2025, the NSC issued a formal advisory warning that “these attacks pose serious risks to the safety of navigation, life at sea, and the marine environment in the region”. Masters and operators are advised to consult Best Management Practices – Maritime Security (BMP-MS) for guidance and to promptly report any suspicious activity or security incidents to the NSC.

The NSC further reports that drifting mines continue to be detected and neutralized by coastal authorities in the southwestern Black Sea.

Masters navigating in the western Black Sea must ensure crews are fully briefed on the potential mines threat. Ships should avoid floating objects, keep the forward area of the ship clear of crew where practicable, and maintain effective visual lookouts at all times. Any sightings of mine-like objects should be reported to coastal authorities, and ships should remain well clear of the hazard. Masters are reminded to monitor local authorities’ broadcasts for the latest navigational warnings, review all relevant NAVAREA III warnings in force, and consult local agents for the most up-to-date operational information.

Operators and masters should maintain contact with their flag administrations to receive the most recent instructions available.

Some coastal states may issue recommended track for ships to follow when arriving or departing from ports. Masters should verify such routing guidance with local agents or port authorities and comply when instructed to do so by the relevant authorities.

AIS should be on at all times. However, note that the NSC assesses the threat of GPS jamming, AIS spoofing, communications jamming, electronic interference and cyber-attacks in the region as high.

Port situation

The United Nations (UN) Black Sea Grain Initiative (BSGI) was terminated in July 2023. Refer to the UN press release of 17 July 2023 for details of the current situation.

Since the termination of the BSGI, Ukraine has established and operates a “temporary humanitarian corridor” to its ports in the northwest Black Sea. See IMO Circular Letter 4748 for details. However, Russia has not indicated its support for this initiative, and has provided no security guarantees, meaning the risks of using the corridor may be higher compared to the BSGI.

Some Ukrainian Danube ports are reported to be open and operational, but ships and crews may be vulnerable to collateral damage from drone strikes against port infrastructures. It is also worth noting that the Ukrainian government has advised the IMO that all its ports are at ISPS Security Level 3.

Russian Black Sea ports are generally reported as operational; however, occasional drone strikes may lead to temporary terminal closures and an increase in ISPS Security Levels.

Ukrainian seafarers may not be granted shore leave in Russian ports, but Russian authorities have announced that Ukrainian seafarers can enter Russian ports onboard ships for the purpose of work onboard that ship. However, ships manned by Ukrainian crew have occasionally faced additional scrutiny by Russian authorities and possible interrogation by Russian authorities when calling at Russian ports.

Commercial operations within the EEZs of Turkey, Georgia, Bulgaria and Romania continue, however ISPS Security Level at ports in the region may be raised. Ships trading to Romanian Danube ports may also be vulnerable to collateral damage from strikes against port infrastructures on the Ukrainian side of the border.

Maritime security advice

The situation in the Black Sea remains volatile and subject to rapid change. All ships operating in this region should stay informed and exercise caution. Gard AS [29] recommend:

- Conducting a thorough risk assessment and evaluate appropriate security measures

- Reviewing current NSC, NAVAREA III and other coastal broadcast warnings

- Updating relevant security and contingency plans, including the crisis communication plans

Consulting the latest versions of the shipping association's MISTO and BMP-MS for guidance.

Ensuring seafarers are fully aware of the security threat in their area of trade.

Following designated safe transit corridors and maintaining a heightened state of awareness during transit, including vigilant lookouts for mines.

Ships should also stay updated on guidance provided by their flag administration regarding the conflict and applicable ISPS Code security levels. If such guidance is not received, pursue clarification with the administration. Contact details for maritime authorities by country can be found on the IMO Global Integrated Shipping Information System (GISIS).

The NSC recommends ships to ensure AIS is transmitting at all times when operating in the Black Sea, consistent with provisions of SOLAS and their flag administration, and monitor VHF Channel 16. However, pursuant to IMO guidelines, "if the master believes that the continual operation of AIS might compromise the safety or security of his/her ship or where security incidents are imminent, the AIS may be switched off. The date, location and time the AIS is switched off should be recorded in the ship's logbook together with the reason for doing so and the master should restart the AIS as soon as the source of danger has disappeared".

In the event of an incident or suspicious activity, ships should notify their flag administration, area authorities, and the NSC. Any ships challenged by military vessels should comply fully with their instructions.

It is also worth noting that ATP-02.1 Naval Cooperation and Guidance for Shipping (NCAGS), a NATO document on the interaction between naval forces and merchant ships, may be relevant. While NATO is not a party to the conflict, this document contains valuable information about the many factors to consider when navigating in areas of armed conflict or war.

Ukraine and Russian waters added to JWC listed areas

As a result of the war in Ukraine, all ports in Russia and certain sea areas in the Black Sea and the Sea of Azov was included in the Joint War Committee's (JWC) list of Hull War, Piracy, Terrorism and Related Perils Listed Areas in April 2022. Owners are advised to contact their war risk insurers when calling any port within these regions. The latest version of the JWLA, along with all JWC bulletins and circulars, are available at the JWC website.

The Warlike Operations Area Committee (WOAC), comprising the UK Chamber of Shipping, Nautilus International, and the RMT union, has declared all Ukrainian, Russian and International Waters north of 44°North in the Black Sea as a 'warlike operations area'.

Guard will update the above sections as new information becomes available. In the meantime, we strongly recommend that ship operators and masters trading to ports in the Black Sea make frequent checks with local sources, such as ship agents and Gard correspondents, to ensure they have

access to the most current and reliable security information at all times. An overview of Gard's correspondents is available [here](#). Additional resources are also available via their hot topic page "War in Ukraine", which provides an overview of Gard's relevant loss prevention material and links to some useful external websites and guidelines to help ship operators, masters, and crews to stay alert and prepared for operations in the Black Sea region. [29]

CONCLUSION

In conclusion, the protection of critical infrastructure (CI) in the maritime environment is a complex and multifaceted challenge that requires a comprehensive and collaborative approach. While the pursuit of perfect protection may be unattainable, governments and organizations should prioritize increasing the resilience of CI against evolving threats. This can be achieved through the adoption of flexible and adaptable strategies that focus on mitigating risks, ensuring continuity of operations, and facilitating swift recovery from disruptive events.

This strategic approach for the Black Sea region will govern the EU initiatives and policies furthering security and democratic resilience, inclusive and sustainable growth, and improved connectivity for the EU and its Black Sea partners through mutually-beneficial partnerships.

The EU will implement the new strategic approach to the Black Sea in synergy with the enlargement process and the Eastern Partnership policy, which provides a well-established framework for cooperation. Engagement and collaboration with strategic partners in the Black Sea region will be reinforced by leveraging the Eastern Partnership actions across all key areas, including people-to-people exchanges and civil society engagement, alongside cooperation on education, culture, youth and gender equality that will provide an important human dimension to the EU's approach.

Finally, the protection of critical infrastructure in the maritime environment requires a collaborative and multidimensional effort. By implementing the recommended measures and focusing on key areas of concern, NATO and its allies can enhance the protection, security, and resilience of critical infrastructure, thus safeguarding societies, ensuring the continuity of essential services, and bolstering the overall security and stability of the alliance and the global system. The recognition that NATO is only as strong as its weakest link should serve as a constant reminder to prioritize the protection of critical infrastructure as an indispensable element of collective security.

REFERENCES

1. Green Paper On A European Programme For Critical Infrastructure Protection, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf
2. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf
3. A Communication on Protecting Europe's Critical Energy and Transport Infrastructure (this document contains sensitive information and is not subject to publication)
4. Green Paper for the Protection of Critical Infrastructure in Ukraine: Analytical Report D. Biriukov, S. Kondratov, O. Nasvit, O. Sukhodolia. - Kyiv. : NISS, 2015. – 33 pages. Electronic version: <http://www.niss.gov.ua>
5. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0135>
6. Critical Infrastructure Facts Page', accessed 3 January 2023, <https://www.networkintegritysystems.com/critical-infrastructure>.
7. Ronald S Bearse, 'Introduction to Critical Infrastructure Security And Resilience (CISR)'.
8. 'NATO 2022 Strategic Concept', accessed 3 January 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pd-f/290622-strategic-concept.pdf.
9. 'NATO 2030: United for New Era', 39, accessed 3 January 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pd-f/201201-Reflection-Group-Final-Report-Uni.pdf.
10. '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 (Text with EEA Relevance)', Text, <https://webarchive.nationalarchives.gov.uk/eu-exit/https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114> (Queen's Printer of Acts of Parliament), accessed 3 January 2023, <https://www.legislation.gov.uk/eudr/2008/114/article/2>.
11. <http://www.niss.gov.ua>
12. Decree of the Cabinet of Ministers of Ukraine dated 23.12.2004 No. 1734 "On Approval of List of Enterprises That Are of Strategic Importance for National Economy and Security"
13. Decree of the Cabinet of Ministers of Ukraine dated 28.07.2003 No. 1170 "On Approval of List of Critical Electrical Power Facilities That Must Be Guarded by Corporate Paramilitary Security in Interaction with Special-Purpose Units of Other Central Executive Bodies"

14. Instruction of the Cabinet of Ministers of Ukraine dated 27.05.2009 No. 578-p "On Approval of List of Critical Oil and Gas Industrial Facilities"
15. Decree of the Cabinet of Ministers of Ukraine No. 1051 dated 15.08.2007 (confidential)
16. Provision on Integrated System for Prevention of, Response to and Suppression of Terrorist Acts and Minimization of Consequences Thereof (approved by the Decree of the Cabinet of Ministers of Ukraine No. 1051 dated 15.08.2007)
17. Decree of the Cabinet of Ministers of Ukraine dated 24.04.99 No. 675-019 "On Approval of List of Objects to be Guarded and Defended in Emergency and During Special Period"
18. Decree of the Cabinet of Ministers of Ukraine dated August 10, 1993 No. 615 "On Measures on Improvement of Security for Assets of State and of Other Type of Property" (with modifications)
19. Law of Ukraine dated 18.01.2001 No. 2245-III "On Extremely Hazardous Facilities"
20. List of Extremely Hazardous Facilities Disruption of Which Requires Special Measures on Prevention of Damage to Lives and Health of the Public, to property, to structures, to Natural Environment / Approved by the Decree of the Cabinet of Ministers of Ukraine dated 06.05.2000 No.765
21. Decree of the Cabinet of Ministers of Ukraine dated 29.08.2002 No. 1288 "On Approval of the Provision on the State Register of Potentially Hazardous Facilities"
22. Order of SNRIU dated 17.12.2012 No. 238 "On Approval of List of Radiological Hazardous Facilities in Ukraine, for Which Facility-Level Design Basis Threat Should Be Developed"
23. Müge M. Akar, Aslihan A. Kemer, and Murat Jane, 'Good Practices in Counter Terrorism in Maritime Domain', Seminar Report (Istanbul, Türkiye: Centre of Excellence Defence Against Terrorism (COE-DAT), 11 October 2022), 3–20.
24. Nedko Dimitrov, Boyan Mednikarov And Valentin Vasilev SECURITY ANALYSIS OF THE NATIONAL MARITIME TRANSPORTATION SYSTEM AS PART OF THE MARITIME CRITICAL INFRASTRUCTURES / 19th Annual General Assembly – AGA 2018 International Association of Maritime Universities (IAMU)
25. EU-Ukraine Solidarity Lanes - European Commission
26. https://transport.ec.europa.eu/document/download/4360ea36-a75a-47e5-8b6f-84a9bde66a02_en?filename=Sustainable_transport_connections_between_Europe_and_Central_Asia.pdf
27. cf. Memorandum of Understanding on a Strategic Partnership in the Field of Energy signed on 18 July 2022

28. Resource https://www.bimco.org/media/1cvf3fu4/bmp-ms_hi-res_s.pdf
BMP Maritime security March 2025
29. Guard. War in Ukraine – impact on maritime situation / Published 28 March 2022
Resource: <https://gard.no/insights/war-ukraine-impact-on-maritime-situation/>