

## Critical maritime infrastructure protection: What's the trouble?

Christian Bueger<sup>\*</sup>, Tobias Liebetrau

University of Copenhagen, Denmark

### ARTICLE INFO

#### Keywords:

Critical maritime infrastructure protection  
Maritime security  
Cyber security  
Nord Stream attack  
Grey zone warfare

### ABSTRACT

The protection of critical maritime infrastructures has become a top political priority, since the September 2022 attacks on the Nord Stream pipelines in the Baltic Sea. This contribution reveals why the protection of infrastructures at sea is a difficult task. Reviewing the spectrum of maritime infrastructures (transport, energy, data, fishing, ecosystems) and the potential threats to them (accidents, terrorism, blue crime, grey zone tactics) demonstrates that designating infrastructures as critical and worthy of special protection measures is a political choice. The analysis moreover shows the need of protective instruments that are tailored to the specificities of maritime space, and the need for integrating diverse policy fields, including defense, diplomacy, marine safety, maritime security and cyber security. Cooperation with the infrastructure industry, enhanced surveillance and investments in repair capacities are also required.

### 1. Introduction: understanding critical maritime infrastructures

The ocean hosts a growing set of infrastructures. If 100 years ago it was shipping lanes, ports and telegraphic cables, the acceleration of oceanic activities [1] has led to a vast growth of infrastructures at sea. The shipping and port industries have experienced significant growth in terms of size and quantity, while a substantial portion of the world's fossil energy supplies are extracted from the oceans or transported through tankers and pipelines. [2] The ocean floor houses millions of kilometers of optic fiber data cables, which serve as the foundation for modern digital communication. [3] The expansion of offshore wind farms, as part of the green energy revolution, has led to the development of new installations at sea, and a rising number of subsea electricity cables. [4]

Contemporary economies and societies are fully dependent on maritime infrastructures. Trade, supply chains, energy and food security rely on them. This is why these infrastructures are often described as 'critical' to the functioning of societies. They are seen as objects that require particular forms of protection, often in the frame of security policies or even by military forces. This is at the heart of the intensifying debate on 'critical maritime infrastructure protection'.

How critical maritime infrastructures, such as ports, can be protected and their security and resilience can be improved, is a key concern on the maritime security agenda. [5] Since the terrorist attacks on the United States of September 11th 2001, the debate on maritime terrorism has led to heightened global awareness of non-state threats to ports. [6]

This was answered with protective measures such as the International Ship and Port Facility Security (ISPS) Code of the International Maritime Organization (IMO), which prescribes rules for the protection of ports and ships. [7,8] While such instruments, were primarily aimed at preventing physical attacks from extremist organizations, growing concerns over cyber-attacks have since led to a substantial re-focusing on the vulnerabilities presented by the digitalization and automation of ports and shipping. [9]

Such ongoing measures to improve technical and safety standards for critical maritime infrastructure were not often a topic of public debate or political priority. However, this changed after the September 2022 attack on the Nord Stream pipelines in the Baltic Sea, which exposed the vulnerabilities of maritime infrastructures, including those on the ocean floor. [10] The act of sabotage, carried out by still unknown perpetrators, brought critical maritime infrastructure protection to the forefront of public discourse and turned it into a top political priority. [11] The spotlight is now on the diverse array of infrastructure at sea, particularly those situated on the seabed, like cables and pipelines, that were previously overlooked and deemed "invisible". [12]

The Nord Stream attacks have led to intensifying policy activity and new strategies and plans for protecting maritime infrastructures in Europe, in particular by NATO and the European Union. Yet, policy actors continue to struggle to identify integrated approaches to critical maritime infrastructure protection. This contribution demonstrates what makes it so difficult to protect critical maritime infrastructures and why policy makers and strategists struggle to find coherent solutions.

<sup>\*</sup> Corresponding author.

E-mail address: [christian.bueger@ifs.ku.dk](mailto:christian.bueger@ifs.ku.dk) (C. Bueger).

<https://doi.org/10.1016/j.marpol.2023.105772>

Received 15 May 2023; Received in revised form 10 July 2023; Accepted 12 July 2023

Available online 15 July 2023

0308-597X/© 2023 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

In the following analysis, the debate on critical maritime infrastructure and the challenges in defining which objects require special protection are discussed. While there is some consensus on what constitutes such infrastructures, political decisions play a significant role in determining their status and scope. Moreover, the unique characteristics of the maritime space are often overlooked in current discussions, which tend to focus on national and terrestrial infrastructure. Furthermore, a review of the various threats to maritime infrastructure is presented and the challenges that the proposed strategies for their protection are facing discussed. While the analysis takes its examples from the European debate, the insights have broader implications for the global debate on critical infrastructure protection.

## 2. The concept of critical maritime infrastructures

Concepts of critical infrastructure have been proposed since the late 1990 s, and critical infrastructure protection is a major issue within security debates since the early 2000 s to the latest. [13,14] Strategies by the European Union and the United States published in 2008 and 2009 have set much of the tone of the debate. [15] Starting out from these, plans, strategies and definitions have flourished across the world. In their majority, the emphasis of critical infrastructure protection is on national and terrestrial infrastructures, and civil protection and engineering solutions. Only marginal attention was given to maritime infrastructures and transnational interdependencies.

Despite these efforts, critical infrastructure, continues to be a concept that is weakly defined. To start with the notion of ‘infrastructure’ is a term difficult to narrow down. [16] The concept finds its origins in planning railroads in the 19th century, but has only come into common usage in policy debates in the 1950 s [17] The term has gradually sunk into colloquial language, but remains contested.

Everyone might agree that an electricity grid or a pipeline can be seen as an infrastructure. Yet, if and how, for instance, the laws and standards regulating these, or the workers that repair and maintain them, should be equally treated as part of an infrastructure, remains controversial. [18] Whether the institutions and maintaining practices, required to run an infrastructure, can be disentangled from the material object is not easy to be addressed. If these are included in the definition, however, the concept of infrastructure becomes so expansive, that it risks becoming a catch-all term or even buzzword.

Adding the term ‘critical’ to the definition does not necessarily solve the problem, but further blurs the definition. [19,20] In this context ‘criticality’ usually refers to the degree that the functioning of a society is dependent on the infrastructure.

The European Union, for instance defines a critical infrastructure as “an asset, system, or part thereof [...], which is essential for the maintenance of vital societal functions, health, safety, security, economic or well-being of people, and the disruption or destruction of which would have a significant impact [...], as result of the failure to maintain those functions.” [21]

The European Union’s definition, is a telling example for how expansive, abstract and generic definitions of criticality are. It is hard to imagine what could, in principle, not be included under such a definition. The focus of critical infrastructure protection, hence, firstly becomes dependent on the methodologies of how one might identify and measure what is ‘essential’, ‘vital’ or a ‘significant impact’.

Methodologies for the identification and designation of critical infrastructures have become more and more sophisticated. [22-24] Yet, methodological refinement does not solve the problem of ambiguity. Any assessment will always be based on value judgements and changing political priorities of what is more or less ‘essential’, ‘vital’ and ‘significant’ – to stay in the European terminology. In other words, critical infrastructure definitions are highly dependent on political choices, rather than technical standards alone.

### 2.1. Types of critical maritime infrastructures

There are different ways of how the debate on critical infrastructures is organized. An established way is to distinguish between different ‘sectors’. [25] While outlines for such sectors tend not to explicitly consider the oceans, five types of maritime infrastructure are often included in the discussion (see Fig. 1):

First, *shipping*: Often considered as part of the transport sector, this infrastructure includes port facilities, the installations used for transport, such as LNG terminals, but also the more invisible shipping lanes, traffic separation schemes, lighthouses, and navigational zones required for maritime safety. [26] Also ships, their construction and maintenance can be included in this type.

Second, *energy*: This comprises of fixed installations at sea, such as oil and gas platforms, windfarms and (planned) energy islands. It also includes the infrastructures through which energy flows to the land, such as underwater pipelines and electricity cables and their connecting points on shore. Since many energy resources, in particular fossil fuels are transported by ships there is a direct connection to the transport sector.

Third, *communication*, that is, the optic fibre cables laid on the ocean floor through which digital data flows and on which the internet is based, as well as the landing stations through which they connect to their terrestrial counterparts. Up to 90 per cent of transcontinental data is transiting through the cables, and countries without terrestrial connections, such as islands, are fully dependent on them. [27]

Fourth, *fishing*, can be seen as part of a ‘food supply sector’. Here ports for fishing, fishing vessels, aquaculture farms come into focus, as well as the management of fishery zones. Fishing can be a substantial industry in coastal regions or for small island states, often crucial in food security, and can hence likewise be seen as critical for societies. [28]

Fifth, *marine biodiversity*: Biodiversity, eco-systems, and ‘nature’ are not necessarily considered to be part of a separate sector in critical infrastructure protection strategies. [29,30] Given that for many countries marine ecosystems are vital for the economy and the population [31], marine biodiversity can be included in an encompassing outline of critical maritime infrastructure. This dimension is moreover gaining in importance, given the heightened awareness of the importance of coastal areas and the seabed as a carbon sink and its potential for carbon storage, which are vital in climate change mitigation and the reduction of carbon emissions. [32]

If and how these five types of infrastructures are included in definitions of critical maritime infrastructure, or potentially others [33], highly differs across countries and regions. In particular in early debates on critical infrastructure protection the focus has been on maritime transport and energy, especially ports. The two latter types, fishing and marine biodiversity, are less regularly included in the debate and many industrial states will consider these as marginal and prefer treating them in different policies. In other contexts, such as least developed states or small island states, however, such infrastructures can be so essential for the national blue economy and food security that they have to be included. It is also expected that the intensifying climate change debate will lead to a re-evaluation of the criticality of such ‘nature’-infrastructures in the light of their role in reducing carbon emissions.

### 2.2. Inter-dependency of infrastructures

Like other types of infrastructures, maritime infrastructures also exhibit a strong interdependence. Ports, for instance, can be crucial nodal points, not only for maritime transport, but also for ensuring energy supplies or for maintaining data and electricity cables. As an example, in Europe the port of Marseille serves not only as a crucial transportation hub, but also accommodates data cable landing stations and cable repair vessels. On the seabed, electricity and data cables cross. Fishing activity and anchoring frequently cause damage to underwater cables [34], and windfarms might lead to accidents with merchant






		On the sea	In the sea	On land
	<b>Transport</b>	Ships, shipping lanes,	Emissions	Ports
	<b>Energy</b>	Platforms	Platforms, electricity cables, pipelines	Ports, landing stations, repair facilities
	<b>Communication</b>	Repair ships	Data Cables	Landing stations, repair facilities
	<b>Fishery</b>	Ships, fishing zones	Fishing gear, aquaculture	Ports, aquaculture
	<b>Eco-systems</b>	Biodiversity	Biodiversity, carbon sink, carbon storage	Coastal areas, beaches

Fig. 1. Types of Maritime Infrastructure.

Source: Own graph.

vessels. An oil spill in a port, could lead to major delays in repairing an underwater cable, if the repair vessel is not able to leave due to pollution. What happens at one infrastructure can hence have direct consequences for the other.

In certain sea regions, the interdependencies can become especially pronounced when there is a dense concentration of maritime infrastructures. The North Sea, Baltic Sea or the South China Sea, for instance, are highly congested maritime spaces. The level of maritime activity not only implies higher risks for accidents, but also competition over ocean space between maritime infrastructures. The Red Sea or Strait of Malacca, for instance, are not only chokepoints for maritime transport, but also the main route for data cables connecting Europe and Asia. In future, congestion is likely to increase due to the ongoing expansion of wind farms, planned energy islands, but also intensified laying of data and electricity cables and hydrogen pipelines. Projected strategies for the North Sea, for example, indicate that wind energy capacities are expected to increase by a factor of 15. [35] Plans to embed aquacultural farms in such installations will further enhance that complexity.

### 2.3. Beyond terrestrial thinking: how maritime infrastructures differ from those on land

Maritime and terrestrial infrastructures are often dealt with by the same policies or within the same strategies. There are, however, fundamental differences, which imply that maritime infrastructures require specific and tailored protection. Three features of maritime space, require particular attention.

First, the majority of critical maritime infrastructures involve a high level of legal complexity. The UN Convention on the Law of the Sea (UNCLOS) is the most fundamental legal regime. [36] According to UNCLOS, maritime infrastructures are situated in different zones, which gives countries particular legal rights and responsibilities. The most important ones are the territorial waters (12 nautical miles), in which countries have full jurisdiction, the Exclusive Economic Zones (200 nautical miles) in which countries have limited legal authority mainly pertaining to economic exploitation and environmental protection, and the high seas, where regulatory powers of states are very limited. It is a particular feature that many maritime infrastructures cut across these zones. This is clearly the case for marine transport, but also for the majority of underwater cables and pipelines that are international connectors.

If shipping is included under the concept of critical infrastructure protection, the picture further complicates, given that ships are governed under the flag state principle of UNCLOS. Ships are under the

jurisdiction of the state to which they are flagged, limiting the legal authorities of coastal and port states. Several other legally binding conventions including by the IMO, such as the ISPS Code, the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (SUA PROT) or the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA) govern maritime infrastructures. Depending on countries and regions, a plethora of additional environmental or sector specific laws are relevant as well. [37] While no systematic comparative analyses have been undertaken yet, often the rules and regulations that apply to maritime zones, differ considerable to those on land.

Second, the sea is a particular geo-physical environment. Maritime conditions, including fluidity, the effect of weather and waves, but also the sheer vastness of ocean space, imply that infrastructures are more difficult to build, to maintain and to protect. The maritime, moreover, is a multi-layered, three-dimensional space and infrastructures are on the sea, in the sea, or on the ocean floor, but many cut across these dimensions. [38]

Repairing failures is more costly, requires specialized equipment with limited availability and is highly weather dependent. Repair times can hence be substantially longer than those on land. Given there is less human activity at sea, and the scale of oceanic space, also surveillance is more difficult. If one includes underwater infrastructure, then these issues become even more prevalent, since in contrast to the surface, the subsea cannot be effectively monitored from the air or the maritime surface.

Third, the majority of maritime infrastructures are transnational: they connect or operate across more than one country. This is the most obvious for shipping given the main purpose of it is the trade between nations. Also, the vast majority of data and electricity cables tend to pass through more than one country's jurisdiction. This implies that countries need to collaborate in the protection of infrastructures through which they are connected. Protection of infrastructures at sea is hence highly dependent on the overall quality of relations between states, and if and how diplomatic relations consider infrastructures.

The unique circumstances of the maritime environment suggest that specialized measures for protecting maritime infrastructure are necessary, which may differ significantly from those employed on land. Therefore, the application of terrestrial-based approaches to maritime infrastructure protection may pose a significant obstacle in developing suitable protective measures. The only exception in this regard is the cyber security dimension, which cuts across land and sea.

### 3. Threats to critical maritime infrastructures

Critical maritime infrastructures are endangered by a multifaceted and intricate range of threats, encompassing not only those identified by the maritime security agenda [39], but also incidents resulting from natural disasters and accidents. The latter can have considerable repercussions on their own or exacerbate the severity of maritime security threats.

Historically, the main focus of critical maritime infrastructure protection debates has been on terrorism. However, in the 2010 s, there has been a shift towards addressing cyber threats. [40] The most recent discourse places significant emphasis on hybrid threats, which may involve intentional actions by hostile states. [41,42]

The threat landscape can be systematically categorized based on two criteria. The first criterion is whether the harm caused is intentional or unintentional. The second criterion encompasses the identity of the perpetrators involved, including state actors, terrorist organizations, criminal networks, or everyday marine users. However, the categorical framework may become intricate due to the emergence of hybrid threats, which entail a fusion of various categories. Fig. 2 provides an overview of the spectrum of threats, with intentional acts that can be addressed through deterrence [43] on the one side, and unintentional events which require resilience measures [44] on the other. We discuss each type of threat in further detail next.

#### 3.1. Unintentional harms

Harm to critical maritime infrastructures can arise from unintentional causes, such as natural disasters like volcanic eruptions, submarine slides, seaquakes, or extreme weather events. For example, in 2022 a volcanic eruption cut the Pacific Island of Tonga from the internet, since all undersea cables were destroyed in the event. [45]

While natural disasters cannot be prevented, another aspect that leads to harm is marine accidents caused by factors such as weather, negligence, or lack of maintenance. Shipping accidents, for example, occur frequently and can result in the shutdown of critical infrastructures, as exemplified by the Evergreen accident in the Suez Canal in 2021. [46] Additionally, underwater cables are often damaged by fishing activities or anchoring, contributing to a significant proportion of annual cable faults. [47]

#### 3.2. Deliberate acts

Deliberate acts of sabotage or disruption can in principle be carried out by states, terrorists, or criminals. The international and national laws under which such activities are governed differ substantially, and hence it is useful to separate out the discussion.

Threats from states are generally associated with scenarios in which

infrastructures become the intentional targets of military action during war. They may also involve situations in which states prepare for war, or when land-based conflict affects the maritime domain. For example, the wars in Ukraine [48] or Yemen [49] have resulted in various navigational hazards, such as floating mines, which pose risks to marine transport well beyond the coastlines of the two countries.

Terrorism threats in the maritime sector are focused on scenarios where extremist organizations aim to attack or disrupt maritime infrastructures for political or symbolic gains. Previous incidents have included attacks on maritime transport and passenger vessels, as well as on ports. [50] No incidents are known in the public domain of extremist organizations deliberately targeting marine energy installations, cables or pipelines, although this continues to be a threat scenario. [51]

The nature of threats posed by blue crime exhibits significant variation. [52] Rather than involving physical destruction or sabotage, such threats tend to be of a disruptive character. For instance, acts of piracy and armed robbery in maritime zones such as the Gulf of Guinea, Strait of Malacca, or off the coast of Somalia, can significantly impede maritime transport flows. Similarly, smuggling activities can create significant disruptions to marine transport, such as when migrant smuggling poses navigational hazards or when suspected narcotics smuggling causes delays in ports. Moreover, if the definition of critical maritime infrastructure protection is expanded to include fishing and marine biodiversity, then the range of environmental crimes, including illegal fishing and deliberate pollution, must be included within the threat landscape.

#### 3.3. Cyber threats

In the age of increasing digitalization and automation, threats to maritime infrastructures derive not only from physical damages caused by sabotage, criminal disruption, accidents or natural disasters, they also include a cyber dimension. [53,54]

Critical infrastructures are highly vulnerable to cyber attacks, which can target either their operating systems or their connectivity. Such attacks can have different objectives: while they may aim to deliberately disrupt the infrastructure, they may also serve to facilitate various types of criminal activities. For example, hackers can exploit vulnerabilities in port systems to facilitate theft or smuggling operations. Similarly, disrupting navigational aids used in shipping (e.g., the Automatic Identification System) can be used as part of criminal operations, including piracy or smuggling.

The inadvertent impact of cyber threats on infrastructures can also result from collateral damage, whereby infrastructures that were not initially targeted are affected. The NotPetya incident serves as a prominent illustration of this, whereby an attack on the Ukrainian electricity infrastructure resulted in the disruption of the digital systems of the major container shipping corporation A.P. Møller – Mærsk A/S. [55]

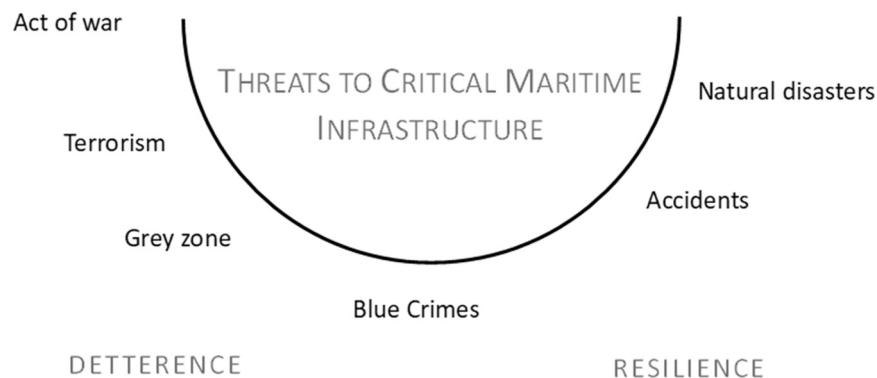


Fig. 2. Threats to Critical Maritime Infrastructure.  
Source: Own graph.



### 3.4. Hybrid threats and grey zone warfare

The concepts of hybrid threats and grey zone warfare are increasingly relevant in critical infrastructure protection. [56,57] These terms refer to situations where states use disruptive measures that fall below the threshold of direct military actions, making it difficult to attribute them directly to a government. Such activities may be intentionally obscured or camouflaged as accidents or the actions of non-state actors. For instance, fishing vessels might be used for such political purposes, or a deliberate disruption might be clouded as an accident. This often creates a high level of uncertainty and ambiguity over the true nature and source of an event, making it challenging to accurately assess the situation and formulate an effective response.

The attack on the Nord Stream pipelines in the Baltic Sea in the Exclusive Economic Zones of Sweden and Denmark that occurred in September 2022 is a paradigmatic example. Observers concur that the incident's high level of sophistication suggests either state sponsorship or some form of governmental backing. However, the precise methods and the identity of the attackers remain unknown, leading to a variety of narratives and theories. [58] Another example are the recurring cable cuts off the coast of Taiwan which have raised concerns whether these incidents are accidental or deliberate acts of political signaling. [59] These examples highlight the challenge of attributing responsibility in situations where state-sponsored actions might be deliberately obfuscated or masked as accidents.

Hybrid and grey zone attacks hence blur the categories of deliberate and unintended events. In such scenarios it might be fundamentally unclear whether an event was an accident, a crime, an act of terrorism, or a state sponsored activity.

## 4. After Nord Stream: how to protect maritime infrastructures

Since the Nord Stream pipeline sabotage in the Baltic Sea, there has been a significant political focus on the safeguarding of critical maritime infrastructure. The incident that officials have called a "wake-up call" [60] highlighted the inherent vulnerability of maritime infrastructure and the inadequacy of current protection and response mechanisms. It underscored the potential severity of threats posed by hybrid and grey zone warfare tactics utilized by adversary states, which were previously underestimated. The event has prompted a renewed recognition of the importance of ensuring the security and resilience of critical maritime infrastructure, and the need for more sophisticated and nuanced strategies to effectively address the complex security challenges posed by such threats.

A flurry of political initiatives within Europe and NATO was the consequence. The European Commission devised an action plan, established a coordination group for critical maritime infrastructure protection, and prioritized this issue in the update of the European Union Maritime Security Strategy. [61] NATO responded by organizing military exercises and setting up a new coordination cell. [62] NATO member states such as Germany and Norway deployed patrols and devised new investment plans for maritime capabilities, such as surveillance systems. [63,64]

As already established these responses face the challenge of a) weak definitions, b) the complexity of the marine environment, and c) the broad spectrum of threats that needs to be considered. The next sections investigate why the new instruments and responses are struggling with developing coherent responses. We outline five distinct policy and operational challenges.

### 4.1. Cross-sector integration

The existing strategies for safeguarding critical infrastructure are sector-specific, with maritime transport, energy, communication, fishing, and marine environment each governed by separate policies and regulatory agencies. This fragmentation of responsibilities presents a

significant challenge to achieving coherence and integrated planning across various sectors under a unified critical infrastructure umbrella. Furthermore, the lack of a clear and universally agreed-upon definition of what constitutes critical infrastructure may generate resistance from the various sector policies and agencies that need to be integrated. The legal complexity of maritime space and the need to harmonize national legislations with international law further complicates the picture. As such, achieving a comprehensive and harmonized approach to critical infrastructure protection poses a complex and multifaceted challenge that requires close collaboration and coordination. On a transnational level these issues multiply and call for coordination in and through regional organizations, such as NATO or the European Union.

### 4.2. Competing policy agendas

The challenge of achieving comprehensive and effective critical maritime infrastructure protection is compounded by the presence of competing policy fields and policy integration initiatives. The relations to overall security and defense, maritime safety, but also the agendas of maritime security, cyber security or diplomacy are often ambiguous. This ambiguity can create competition and conflicts between agendas and involved agencies, further complicating efforts to establish a cohesive and coordinated approach.

The traditional security and defense apparatus, in particular focuses on threats from states and terrorism. Here military responses, such as deterrence strategies are strongly favored, which raises questions of how to integrate civilian components. The maritime safety sector in charge for navigation and port state measures is the pre-dominant way of how maritime infrastructures have been regulated in the past. These civilian instruments, often carried out by coast guards and police, are however not necessarily equipped to deal with state-based threats or grey zone scenarios. Yet, they have the most reliable relations to the industry, in particular the fishing and transport sector.

Maritime security and cyber security have advanced in the past decades to a degree that they are more than policy integration initiatives, but increasingly independent domains with separate coordination mechanism or sometimes even agencies. These are relevant in critical maritime infrastructure protection, yet the same time cannot be reduced to these. Lastly, and in so far as critical maritime infrastructures involve the relations between states, protection is, or at least should be, part of the diplomatic agenda in terms of improving safeguards between countries connected by infrastructures.

### 4.3. Industry cooperation

The industries that finance, build, own, operate and maintain maritime infrastructure are perhaps the pivotal actors without which protection cannot work. [65] It is industries and their associations that hold the expertise of how infrastructures precisely function, how they are connected to and dependent on others, what vulnerabilities they face, and what is required to maintain and repair them. Such expertise, including on recent technological advancement, is only to limited degree available among the governmental agencies discussed above.

The majority of operators moreover closely monitor their infrastructures to detect failures or prevent accidents. Industry hence may hold important expertise and information that is required for critical maritime infrastructure protection. This necessitates close collaboration, but also raises the question of how responsibilities and costs should be shared between taxpayers, consumers and industries. The industry might have to employ significant self-protective measures including physical hardening or even private guards. The data collected by industries and how it can be used may moreover raise concerns over privacy and ownership. The creation of new coordination cells, for instance, by NATO [62] and new stakeholder forums [66] are geared towards enabling this cooperation.

#### 4.4. Surveillance and sensors

Over the past decades there have been substantial investments in the surveillance of maritime space in order to improve marine safety and maritime security. Current systems, often known as Maritime Domain Awareness (MDA), are based on ship routing and position data from the Automatic Identification System. [67] Such data on maritime movements is augmented through coastal radars, CCTV, patrols at sea and in the air, and increasingly from satellites and uncrewed vehicles. [68] MDA systems are one of the core solutions in maritime security. They have the goal to increase the speed of incident responses and issuing of early warnings, but also to identify suspicious behaviour, patterns, trends and threats in order to counter-act or prevent them. They do so by fusing data and with the support from machine learning and prospectively artificial intelligence tools. [69]

Effective MDA requires the fusion of different data sources across states and agencies, and also integrating information from industry. Distrust, organizational politics, or divergent data standards can here be difficult to overcome. In Europe, it is in particular the Common Information Sharing Environment which is the key project through which the European Union wants to enhance its MDA. [70]

Current systems are mainly focused on the maritime surface and track vessels of the transport, fishing and travel industry. The surveillance of small boats and leisure crafts is less advanced. Under the sea, current surveillance is severely limited. This is problematic as the main threats might come from underwater vehicles, in particular under grey zone scenarios. Protecting subsea infrastructures, will here imply investments in new underwater sensors and drones which can enhance the overall picture of the domain. In Europe it is in particular the European Defence Agency which is active in this regard. [71] Given the vastness of underwater infrastructures and, for instance, the length of cables systems, a full live monitoring of the infrastructures, however, will be impossible to achieve.

#### 4.5. Maintenance and repair

The final dimension of critical maritime infrastructure protection, maintenance and repair, often receives the least attention. Repair capacities are required to reduce the impact of an infrastructure fault and its potential consequences for related and connected systems. Strong repair capacities also potentially present a deterrence strategy towards grey zone tactics, since the strategic value of an attack is decreased – a strategy known as ‘deterrence by denial’. [72]

Repair capacities are privately owned and often limited because of the underlying cost-value calculations of industries. This implies close cooperation between states and industry in order to develop best practices and exchange experiences and improve information sharing for repair, on the one hand.

It also raises the question if and how governments, for instance, as part of the armed forces can provide supplementary repair capacities. This might be in the form of multi-purpose vessels that can fulfill repair functions in emergency situations. The United Kingdom’s Royal Navy, for instance, has recently acquired a vessel for underwater surveillance that could be task with repair. [73]

### 5. Conclusion

Critical maritime infrastructure protection has become a renewed political priority, especially since the 2022 Nord Stream attacks. Although not entirely new as an agenda, it is now being prioritized and re-examined. In contrast to earlier approaches, the critical importance of green energy installations and underwater systems has come into focus.

The concept of critical maritime infrastructures continues to be weakly defined. Some definitions, such as the European Union’s one, are so vague, that almost anything could be understood as a critical infrastructure. While methodologies for risk assessments and the

identification of vulnerabilities are increasingly improved, designating infrastructures as essential for societies remains primarily a political choice. It follows that the relevance and criticality of infrastructures is a question of context.

In principle five maritime infrastructures need to be considered in the debate: Shipping (ports, navigational aids, ships), energy (oil and gas platforms, wind farms, pipelines and electricity cables), communications (underwater fiber optic cables, landing stations), fishing (aquaculture, fishing ports, vessels, fishing zones), and marine biodiversity (marine ecosystems, marine protected areas). These are highly interdependent with each other.

Current critical infrastructure programmes tend to misconceive the specificities of maritime space by clustering maritime infrastructures in sectors that are conceptualized in terrestrial and often national terms. The legal complexity and transnational character, as well as the particular geophysical conditions of the oceans are thereby often not appropriately considered.

If terrorism and cyber security have dominated much of the early maritime infrastructure protection agenda, in the contemporary geopolitical landscape a much wider spectrum of threats must be taken into account. Tactics of grey zone and hybrid warfare pose a particular challenge since attacks might be clouded as accidents and are difficult to attribute or prosecute.

Integrating the different sectors and related policy fields is difficult to achieve and presents an enormous coordination challenge on a national but also regional level. Coordination between agencies and with the industry, including in surveillance and ensuring appropriate repair and maintenance capacities is also required for effective protection.

The current measures as they are developed in Europe, including by NATO and the European Union, for critical infrastructure regions, such as the North Sea, Baltic Sea, Mediterranean or Atlantic are promising, but they continue to struggle and practical challenges remain. Overall, in rethinking critical maritime infrastructure protection the European organizations are on course to set an important role model of how to achieve resilience and security on a regional level. The future lessons from these activities will hence become important for other regions, such as the Indian Ocean, South China Sea or infrastructure chokepoints such as the Strait of Malacca, Strait of Hormuz or Red Sea.

#### Data Availability

No data was used for the research described in the article.

#### Acknowledgements

This article draws on and advances arguments first presented by Bueger as a keynote speech at the 1st Symposium on Critical Maritime Infrastructure Protection by the European Defence Agency (EDA), Brussels, April 2023. We thank the EDA for the invitation and the participants for the comments and suggestions. Versions of this article have also been presented at an event by the European Council working party on maritime security, Karlskrona, Sweden, June 2023, and the National University of Singapore, Singapore, July 2023. Research for this article has benefitted from a grant by the Velux Foundation for the Ocean Infrastructure Research Group. We are grateful to Robert C. Beckman, Tara Davenport, Tim Edmunds, Brendan Flynn, Jonas Franken, Kimberley Peters, Jan Stockbruegger, Vonintsoa Rafaly, and John Wrottesley as well as the two anonymous reviewers for ideas, comments and suggestions that have improved the manuscript.

#### References

- [1] Magnus Nystro, Jean-Baptiste Jouffray, Robert Blasiak, Albert V. Norstro, The blue acceleration: the trajectory of human expansion into the ocean, *One Earth* 2 (1) (2020) 43–54, <https://doi.org/10.1016/j.oneear.2019.12.016>.
- [2] UNCTAD, *Navigating stormy waters. Review of Maritime Transport*, UNCTAD, Geneva, 2022.

- [3] Jill C. Gallagher, Undersea telecommunication cables: technology overview and issues for congress, *Congr. Res. Serv.* (2022). R47237.
- [4] Global Wind Energy Council, Global Offshore Wind Report, Global Wind Energy Council, Belgium, 2021.
- [5] Christian Bueger, Timothy Edmunds, Beyond seabindness: a new agenda for maritime security studies, *Int. Aff.* 93 (6) (2017) 1293–1311, <https://doi.org/10.1093/ia/iix174>.
- [6] James A. Malcolm, Responding to international terrorism: the securitisation of the United Kingdom's Ports, *Br. J. Polit. Int. Relat.* 18 (2) (2016) 443–462, <https://doi.org/10.1177/1369148115623211>.
- [7] John King, The security of merchant shipping, *Mar. Policy* 29 (2005) 235–245.
- [8] Prakash Metaparti, Rhetoric, Rationality and Reality in Post-9/11 Maritime Security, *Marit. Policy Manag.* 37 (7) (2010) 723–736.
- [9] Orestis Schinas, Daniel Metzger, Cyber-seaworthiness: a critical review of the literature, *Mar. Policy* 151 (2023), 105592.
- [10] Christian Bueger, Tobias Liebetrau, Nord Stream sabotage: the dangers of ignoring subsea politics, *The Loop*, 7.10.2022, <https://theloop.ecpr.eu/nord-stream-sabotage-the-dangers-of-ignoring-subsea-politics/>.
- [11] Alexandra Brzozowski, Kira Taylor, EU vows to draw up plan to protect critical infrastructure, *Euractiv.com*, 5.10.2022, <https://www.euractiv.com/section/defence-and-security/news/eu-vows-to-draw-up-plans-to-protect-critical-infrastructure/>.
- [12] Christian Bueger, Tobias Liebetrau, Governing hidden infrastructure: the security politics of the global submarine data cable network, *Contemp. Secur. Policy* 42 (3) (2021) 391–413.
- [13] Kristin Ljungkvist, Arjen Boin, Protecting Europe's critical infrastructures: problems and prospects, *J. Contingencies Crisis Manag.* 15 (1) (2007) 30–41.
- [14] Christer Pursiainen, The Challenges for European Critical Infrastructure Protection, *Eur. Integr.* 31 (6) (2009) 721–739.
- [15] EU Directive 114/08/EC of 2008 and United States National Infrastructure Protection Plan of 2009.
- [16] Jens Ivo Engels, Introduction. in *Key Concepts for Critical Infrastructure*. Jens Ivo Engels, Springer VS, Wiesbaden, 2018, pp. 1–10.
- [17] Carse, Ashley, Keyword: infrastructure: how a humble french engineering term shaped the modern world. *Infrastructures and Social Complexity: A Companion*, Routledge, Abingdon, 2016, pp. 27–39.
- [18] Christian Bueger, Tobias Liebetrau, Stockbruegger Jan. *Theorizing Infrastructures in Global Politics*, mimeo, University of Copenhagen, 2023.
- [19] Kristof Lukitsch, Marcel Müller, Chris Stahlhut, Criticality, in: Jens Ivo Engels (Ed.), *Key Concepts for Critical Infrastructure*, Springer VS, Wiesbaden, 2018, pp. 11–20.
- [20] Claudia Aradau, *Security That Matters: Critical Infrastructure and Objects of Protection*, *Secur. Dialogue* 41 (5) (2010) 491–514.
- [21] Directive 2008/114/EC, Articles 2 and 3
- [22] Jose M. Yusta, J.Correa Gabriel, Roberto Lacal-Arategui, Methodologies and applications for critical infrastructure protection: state-of-the-art", *Energy Policy* 39 (2011) 6100–6119.
- [23] Josune Hernantes, Jose M Sarriegi, Ana Lauge, *Critical Infrastructure Dependencies: A Holistic, Dynamic and Quantitative Approach*, *Int. J. Crit. Infrastruct. Prot.* 8 (2015) 16–23.
- [24] Simona Esposito, Božidar Stojadinović, Anže Babić, Matjaž Dolšek, Sarifraz Iqbal, Jacopo Selva, Marco Broccardo, Arnaud Mignan, Domenico Giardini, *Risk-Based Multilevel Methodology to Stress Test Critical Infrastructure Systems*, *J. Infrastruct. Syst.* 26 (1) (2019).
- [25] Jose M. Yusta, J.Correa Gabriel, Roberto Lacal-Arategui, Methodologies and applications for critical infrastructure protection: state-of-the-art", *Energy Policy* 39 (2011) 6100–6119, <https://doi.org/10.1016/j.enpol.2011.07.010>.
- [26] Kimberley Peters, Deep routing and the making of 'maritime motorways': beyond surficial geographies of connection for governing global shipping, *Geopolitics* 25 (1) (2019) 43–64.
- [27] Christian, Bueger, Tobias Liebetrau and Jonas Franken, Security threats to undersea communications cables and infrastructure – consequences for the EU, *In-Depth Analysis for the European Parliament* commissioned by the Sub-Committee on Security and Defense, Brussels, 1.6.2022, ([https://www.europarl.europa.eu/thinktank/en/document/EXPO\\_IDA\(2022\)702557](https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557)).
- [28] USAID, *Fishing for Food Security: The Importance of Wild Fisheries for Food Security and Nutrition*, USAID, Washington, D.C., 2016.
- [29] Ashley Carse, *Nature as Infrastructure: Making and Managing the Panama Canal Watershed*, *Soc. Stud. Sci.* 42 (4) (2012) 539–563.
- [30] Connor Joseph Cavanagh, *Critical Ecosystem Infrastructure? Governing the Forests - Water Nexus in the Kenyan Highlands*, in: Rutgerd Boelens, Tom Perreault, Jeroen Vos (Eds.), *Water Justice*, Cambridge University Press, Cambridge, 2018, pp. 302–315.
- [31] Martin Stuchtey, Adrien Vincent, Andreas Merkl, Maximilian Bucher, et al., *Ocean Solutions That Benefit People, Nature and the Economy*, World Resources Institute, Washington, DC, 2020. ([www.oceanpanel.org/ocean-solutions](http://www.oceanpanel.org/ocean-solutions)).
- [32] David A. Siegel, Timothy DeVries, Ivona Cetinić, Kelsey M. Bisson, Quantifying the ocean's biological pump and its carbon cycle impacts on global scales, *Annu. Rev. Mar. Sci.* 15 (2023) 329–356.
- [33] Which might include offshore space ports, bridges, underwater tunnels, deep sea mining, or other sectors of the blue economy, such as recreational industries.
- [34] Christian Bueger, Tobias Liebetrau, Governing hidden infrastructure: the security politics of the global submarine data cable network, *Contemp. Secur. Policy* 42 (3) (2021) 391–413.
- [35] Ostend Declaration by Energy Ministers. 2023. <https://kefm.dk/Media/638179241161947530/7.%20Declaration%20LEADER.pdf>.
- [36] Yoshifumi See Tanaka, *The International Law of Sea*, Cambridge University Press, Cambridge, 2019.
- [37] For a review of applicable law, see, for instance, James Kraska, Raul Pedrozo. 2013. *International Maritime Security Law*, Martinus Nijhoff, Leiden & Boston, 2013.
- [38] Andrew Barry, Evelina Gambino, Pipeline geopolitics: subaquatic materials and the tactical point, *Geopolitics* 25 (1) (2020) 109–142, <https://doi.org/10.1080/14650045.2019.1570921>.
- [39] Christian Bueger, Timothy Edmunds, *Understanding Maritime Security*, Oxford University Press, Oxford, 2024.
- [40] Martti Lehto, Pekka Neittaanmäki (Eds.), *Cyber Security: Critical Infrastructure Protection*, Springer Nature, 2022.
- [41] Christer Pursiainen, Eero Kytömaa, From European critical infrastructure protection to the resilience of european critical entities: what does it mean? *Sustain. Resilient Infrastruct.* 8 (1) (2023) 85–101.
- [42] Eitvydas Bajarūnas, Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond, *European View* 19 (1) (2023) 62–70.
- [43] Julian Pawlak, *Der Schutz Maritimer Kritischer Infrastrukturen Und Das Konzept Der Abschreckung*, *Sirius* 7 (2) (2023) 160–166.
- [44] Christer Pursiainen, Eero Kytömaa, From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean? *Sustainable and Resilient Infrastructure* 8 (1) (2022) 85–101.
- [45] Euronews, Tonga is finally back online. Here is why it took 5 weeks to fix its volcano damage. *Euronews*. 23.2.2022, <https://www.euronews.com/next/2022/02/23/tonga-is-finally-back-online-here-s-why-it-took-5-weeks-to-fix-its-volcano-damaged-interne>.
- [46] Jade Man-yin Lee, Eugene Yin-cheung Wong, Suez Canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain, *MATEC Web Conference* 339 (2021), 01019.
- [47] Mike Clare, *Submarine Cable Protection and the Environment. An Update from the ICPC, International Cable Protection Committee* (2021). [https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC\\_Public\\_EU\\_March%202021.pdf](https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf).
- [48] Euronews, Ukraine war: Drifting mines pose deadly threat in Black Sea waters. *Euronews*. 11.8.2022, <https://www.euronews.com/2022/08/11/ukraine-war-drifting-mines-pose-deadly-threat-in-black-sea-waters>.
- [49] Al-Tamimi, Nabil Abdullah Al-Tamimi, Floating Death': Houthis' Red Sea mines pose lasting threat, *Al-Mashareq*, 10.6.2022, [https://almashareq.com/en\\_GB/articles/cnmi\\_am/features/2022/06/10/feature-03](https://almashareq.com/en_GB/articles/cnmi_am/features/2022/06/10/feature-03).
- [50] Meghan Curran, Christopher Faulkner, Curtis Bell, Tyler Lycan, Michael Van Ginkel, Jay Benson, *Violence at sea: how terrorists, Insurgents, and Other Extremists Exploit the Maritime Domain, Stable Seas and One Earth Future Foundation*, Colorado, 2020.
- [51] Camille Morel, *Threats beneath the Seas: Vulnerabilities in the Global Cable Network*, *Herodote* 163 (4) (2016) 33–43.
- [52] Christian Bueger, Timothy Edmunds, *Blue Crime: Conceptualising Transnational Organised Crime at Sea*, *Mar. Policy* 119 (2020), 104067.
- [53] Orestis Schinas, Daniel Metzger, *Cyber-Seaworthiness: A Critical Review of the Literature*, *Mar Policy* 151 (2023), 105592.
- [54] Mawuli Afenyo, Livingstone D. Caesar, *Maritime cybersecurity threats: Gaps and directions for future research*, *Ocean and Coastal Management* 236 (2023), 106493.
- [55] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, *Wired*, 22.8.2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- [56] James Goldrick, *Greyzone operations and the maritime domain*. Australian Strategic Policy Institute, 2018.
- [57] Andrew S. Erikson, ed., *Maritime Gray Zone Operations Challenges and Countermeasures in the Indo-Pacific*, Routledge, Abingdon, 2023.
- [58] Christian Bueger, *Russian Spy Ship in North Sea raises concerns about the vulnerability of key maritime infrastructures*, *The Conversation*, 20.4.2023, <https://theconversation.com/russian-spy-ship-in-north-sea-raises-concerns-about-the-vulnerability-of-key-maritime-infrastructure-204205>.
- [59] Rachel Cheung, *A warning Sign': Chinese Ships Accused of Cutting off Internet to a Taiwanese Island*, *Vice News*, 17.3.2023, <https://www.vice.com/en/article/byj8x3/taiwan-internet-cables-matsu-china>.
- [60] Richard Milne, Henry Foy, Sheppard David, *Sabotage of gas pipelines a wake-up call for Europe, officials warn*, *Financial Times* (29.9.2022). <https://www.ft.com/content/ad885fea-035f-4b93-98e7-c75da2c308f8>.
- [61] European Commission. *Joint communication on the update of the EU Maritime Security Strategy and its Action Plan: An enhanced EU Maritime Security Strategy for evolving maritime threats*, JOIN/2023/8, European Commission, Brussels, 2023.
- [62] NATO, *NATO stands up undersea infrastructure coordination cell*. *NATO News*, 15.2.2023, [https://www.nato.int/cps/en/natohq/news\\_211919.htm](https://www.nato.int/cps/en/natohq/news_211919.htm).
- [63] Frank Umbach 2023. *New challenges in protecting critical EU infrastructure*. *GIS Reports* (2023), <https://www.gisreportsonline.com/tr/europe-critical-infrastructure-re/>.
- [64] Julian Pawlak, *Der Schutz Maritimer Kritischer Infrastrukturen Und Das Konzept Der Abschreckung*, *Sirius* 7 (2) (2023) 160–166.
- [65] Chris Koski, *Committed to Protection? Partnerships in Critical Infrastructure Protection*, *J. Homel. Secur. Emerg. Manag.* 8 (1) (2011) 1–18, <https://doi.org/10.2202/1547-7355.1860>.
- [66] European Defence Agency. 2023. *EDA Symposium. Critical Maritime Infrastructure Protection*, European Defence Agency, 16.2.2023. <https://eda.europa.eu/news->

- and-events/events/2023/04/27/default-calendar/eda-symposium-critical-maritime-infrastructure-protection.
- [67] Christian Bueger, A glue that withstands heat? The promise and perils of maritime domain awareness, in: Edward R. Lucas, Samuel Rivera-Paez, Thomas Crosbie, Felix Falck Jensen (Eds.), "Maritime Security: Counter-Terrorism Lessons from Maritime Piracy and Narcotics Interdiction", 235–245, IOS Press, 2020.
- [68] Gregory B. Polling From Orbit to Ocean — Fixing Southeast Asia 's Remote-Sensing Blind Spots" Naval War College Review 74, 1 (2021) Article 8.
- [69] Chamali Gamage, Dinalankara Randima, Samarabandu Jagath, A comprehensive survey on the applications of machine learning techniques on maritime surveillance to detect abnormal maritime vessel behaviors, 6.2023, WMU J. Marit. Aff., Online first 27 (2023), <https://doi.org/10.1007/s13437-023-00312-7>.
- [70] Tikanmäki, Ilka. 2017. Common Information Sharing on Maritime Domain. - A Qualitative Study on European Maritime Authorities Cooperation, Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management - Volume 3: ISE, 283–290.
- [71] European Defence Agency. 2023. Capability Development: Sea. <https://eda.europa.eu/what-we-do/capability-development/sea>.
- [72] Alex S. Wilner, Andreas Wenger, Deterrence by Denial: Theory and Practice, Cambria Press, 2021.
- [73] UK Royal Navy, Navy's new guardian of key underwater infrastructure arrives in UK. Royal Navy News, 19.1.2023, <https://www.royalnavy.mod.uk/news-and-activity/news/2023/january/19/20230119-navys-new-guardian-of-key-underwater-infrastructure-arrives-in-uk>.