The new Frontier of Maritime Domain Awareness: Lessons from Europe's Experience in Critical Maritime Infrastructure Protection

Christian Bueger, *University of Copenhagen & SafeSeas*

June 2024

Maritime Domain Awareness is one of the most important tools in the repertoire of maritime security solutions. Getting a real time picture of activities at sea through fusing data from different sources, allows for more effective law enforcement and the prevention of spirals of insecurity at sea.

This contribution argues that MDA has been significantly advanced but remains too focused on the surface. Integrating the subsea, airspace, low orbit and cyber domain in MDA is the next frontier and vital for critical maritime infrastructure protection. This task has become a priority in Europe. Drawing on the European experience leads to the identification of six major challenges in extending MDA for critical maritime infrastructure protection.

The global evolution of MDA

MDA system are getting more and more sophisticated. Centers are now operational across the world. Regional coverage is increasingly achieved, except for the South Atlantic. Regional centers have consolidated their work and organizational procedures and made important steps to enhance their inter-operability. The relationships to maritime stakeholders, such as the shipping industry, are improving. Also, the social barriers to information sharing are now well recognized, and digital tools for decision support are getting more and more advanced. MDA has become a global project, and it is increasingly working to address threats and challenges.

The same time, MDA so far is firmly focused on surface activities. It tracks and monitors the behavior of vessels on the surface and neither pays much attention to what happens above nor under the sea. While many maritime activities are on the surface, paying attention to the subsea, airspace and low orbit is vital, too.

The new frontier of MDA

Many regional seas, such as the North Sea or South China Sea have become heavily industrialized ocean spaces. All sorts of installations are placed at sea, with energy installations the most visible. Oil and gas platforms, offshore renewable energy sources rely on the transmission of energy

through underwater pipelines and cables. The seabed also hosts the optical fiber cables through which the global internet runs. The space above the sea is equally important. Not only can the airspace be used to launch attacks on shipping, but navigation and maritime surveillance are increasing dependent on low orbit satellites. Lastly, the maritime domain is also closely interwoven with the digital realm. Automation and digitization mean that maritime security also needs to integrate the cyber security agenda.

Integrating these features in maritime domain awareness is the next frontier of MDA. Paying attention to them is vital to protect not only shipping, but also all the other critical maritime infrastructures. Specifically, wind energy expansion is vital for decarbonization and making the green energy transition happen. This will alter the face of many regional seas fundamentally.

The more dependent societies become on maritime infrastructures, the more these are vulnerable, as recent acts of deliberate sabotage on pipelines in the Baltic Sea document.

The European experience

The need to widen the focus of MDA has become a policy priority in Europe since countries have been most immediately affected by recent attacks and have started to recognize the vulnerabilities under and above the sea.

What measures have European countries taken to incorporate the critical maritime infrastructure protection agenda? What are the challenges that become visible in these activities?

I review the responses by NATO and the EU as well as a range of other initiatives, and then identify six challenges that come to the fore. The European initiatives hold important lessons for integrating critical maritime infrastructure protection in MDA in other regions.

EU and NATO responses

In response to the Nord Stream pipelines attacks of September 2022, both the European Union (EU) and NATO have upscaled their MDA activities.

The EU has included critical maritime infrastructure protection as a priority in its October 2023 European Maritime Security Strategy. It attempts to integrate infrastructures in its two key MDA activities, (1) the Common Information Sharing Environment (CISE) which connects all of the 400 European agencies with coastguard functions under one system operated by the European Maritime Safety Agency (EMSA), and the military component of CISE called MARSUR operated by the European Defense Agency (EDA). With EDA in the lead the EU is also organizing tabletop exercises on information sharing or critical maritime infrastructure protection, including an exercise on the North Sea held in May 2024. In February 2024 the European Commission has also initiated a new member state expert group which develops guidelines for the protection of subsea cables and aims to advance information sharing on the issue.

NATO started to work on solutions for critical maritime infrastructure protection immediately after the Nord Stream attacks. It had warned about risks and vulnerabilities in this domain for a while. Its two key responses became operative in May 2024.

NATO's Maritime Centre for Security of Critical Undersea Infrastructure is based in the Maritime Command and aims at working with member states and industry to conduct an assessment of vulnerabilities, to introduce a reporting mechanism and develop tactical responses. NATO's Critical Undersea Infrastructure Network is a cooperation with industry. Both initiatives have as their key focus to deter attacks by developing capabilities to attribute incidents to state adversaries.

Other initiatives

While the EU and NATO focus their work on the entire sea space they consider to be of interest and to some degree take a global approach, another initiative is focused on one regional sea: The North Sea. Initiated by the Belgian government, in *the Joint Declaration on cooperation to secure critical subsea infrastructure* the North Sea states have agreed to strengthen cooperation and information sharing and are building a new MDA platform focused on maritime infrastructures. The new system NorthSeal is expected to be operational in October 2024. A core feature of the platform is reporting of suspicious activities, such as from spy vessels.

On a national level, countries such as Belgium, France, Italy and the United Kingdom have been particularly pro-active. Belgium has introduced a new law for its maritime domain and experiments with CCTV, drones, 5G and other sensing systems many of which are installed on wind energy platforms to enhance MDA. France implements a naval strategy for the seabed which largely focuses on military capabilities. Italy has introduced a naval program which focuses on legal review, new sensors, as well as close coordination with industry. The United Kingdom's Royal Navy has acquired a vessel with which it experiments how to better monitor threats in the underwater domain, and is developing a reporting system for suspicious events under its Joint Maritime Security Center.

Six major challenges become visible in this impressive range of activities.

Challenge 1: Mapping Infrastructure at Sea

European countries have recognized that they lack a comprehensive understanding of what infrastructures are based in the areas under their jurisdiction and how they are connected to other countries outside these. One of the priority activities of the initiatives described above is hence to gather a comprehensive mapping of current and planned infrastructures

Such a mapping is only possible in close collaboration with marine spatial planning (MSP) and ocean observatory projects and activities, which are compulsory in the European Union. Yet, this is challenging since MSP is focused on the blue economy and ocean health, and there is a limited track record of working with maritime security agencies.

Challenge 2: What is critical?

The scale and extent of maritime infrastructures (however defined) is enormous. Thousands of kilometers of cables and pipes lay on the sea floor, and the number of offshore installations grows continuously. This implies the need to prioritize which parts of infrastructures should see higher levels of protection. The identification of vulnerabilities and criticality, however, cannot draw on agreed definitions and standards. Measuring criticality hence remains a major challenge.

Challenge 3: Reporting of suspicious behavior

Threats to critical maritime infrastructures are diffuse and difficult to assess. Outside clear cut damage from extreme weather or from direct military attack, the majority of threats are in the grey zone or hybrid spectrum, where it will be always difficult to assess whether an incident is deliberate or an accident.

The diffuse nature implies that the understanding of suspicious behavior needs to be casted widely. Any activity might be part of a pattern and become only suspicious if that pattern is known. That raises the question of which observations precisely should be reported in the new systems.

Challenge 4: Industry and governments

A third challenge concerns how governmental maritime security agencies can work most productively with industry and can develop trust information sharing and reporting system. This is a general challenge of MDA. Yet, under the critical maritime infrastructure agenda, MDA has to work with other industry sectors than transport – sectors with which many MDA centers have not developed relations in the past.

This includes the offshore energy industry and communication industry. Both industries already monitor their assets at sea closely. This data can be important information in MDA yet raises the question if and how industries should be requested to report mandatory. Other platforms do not have installed sensors, which raises the question of whether industry should be required to install these. If such sensors are military, rather than civilian in character, risks may arise that installations become targets.

Challenge 5: Which new technologies?

A floury of new technologies is currently developed. This ranges from new autonomous surveillance drones in the air space, surface and subsea domains, and expansion of satellite observations, 5G surveillance, to better and stronger cameras.

Many of these technologies are in an experimental stage, and overall, they are expensive. To advance to the next stage of MDA, significant decisions must be made regarding which technologies to prioritize and the associated investment costs. Additionally, it raises the issue of whether these costs should be borne by taxpayers, consumers, or shareholders.

Challenge 6: Fragmentation

As the short review of MDA activities in Europe focused on critical maritime infrastructures reveals, there is hardly a coherent European approach. Initiatives are either civil or military in character, they are focused on a particular regional sea, or are cross-regional or even global in scope. Some states prefer national over regional solutions. Preventing duplication and competition and ensuring that the fragmentation implied by the multiple initiatives is hence another challenge.

Beyond Europe: Critical Maritime Infrastructure Protection is a global task.

While the maritime security context in Europe differs from other parts of the world, the need to protect critical maritime infrastructure is a global task. All nations depend on subsea data cables for their digital connectivity, the expansion of offshore green energy infrastructures, for instance, in Sri Lanka, Southern India, or Vietnam, is progressing rapidly, and new electricity cables connect nations of the world. The European experience will be important in developing solid MDA solutions for addressing the vulnerabilities that come with it. Finding cooperative, cost-efficient solutions and addressing the challenges outlined above, is hence the new frontier of MDA.

Christian Bueger is a professor at the University of Copenhagen and a research fellow at the United Nations Institute for Disarmament Research (UNIDIR). He is the author of Understanding Maritime Security (with Tim Edmunds) published by Oxford University Press. He can be contacted at Christian.bueger@ifs.ku.dk and further information is available at www.bueger.info .

Related literature

Bueger, Christian and Tim Edmunds. Maritime security and the wind: Exploring threats and risks to renewable energy infrastructures offshore, Ocean Yearbook 39, 465-488, 2024, http://dx.doi.org/10.13140/RG.2.2.23647.64167

Bueger, Christian. NATO's contribution to critical maritime infrastructure protection, The MOC, Institute for Maritime Strategy, 19.1.2024, https://centerformaritimestrategy.org/publications/natos-contribution-to-critical-maritime-infrastructure-protection/

Bueger, Christian. Beyond Surface. The six spatial domains of maritime security, KIMS Periscope, 11.1.2024, Korea Institute for Maritime Strategy, https://kims.or.kr/issubrief/kims-periscope/peri336/ .

Bueger, Christian. Why Southeast Asian nations must better protect their critical maritime infrastructures, The Diplomat, 8.8.2023, https://thediplomat.com/2023/08/why-southeast-asian-nations-must-do-more-to-protect-their-critical-maritime-infrastructure/ .

Bueger, Christian and Tobias Liebetrau. Critical Maritime Infrastructure Protection: What's the trouble?, Marine Policy 155: 105772, 2023, https://doi.org/10.1016/j.marpol.2023.105772