

The New Maritime Security Law

Belgian Navy's role in the legal shield for protection of critical infrastructure



Multipurpose frigate *Louise-Marie* (source: Belgian Navy)



In June 2023, Dmitry Medvedev, Vice-President of the Security Council of the Russian Federation and former President, made a startling statement: 'If we proceed from the proven complicity of Western countries in undermining the Nord Streams, then we have no moral restrictions left to refrain from destroying the cable communications of our enemies laid along the ocean floor.' The Nord Stream sabotage served as a resounding political wake-up call, resonating at the national, EU, and NATO levels. Medvedev's statement underscored the vulnerability of the critical infrastructure lying on the seabed. Although seabed warfare is not a novel concept¹, the convergence of technological developments, our increasing dependence on such infrastructure, and the growing accessibility of technologies like underwater drones have significantly elevated the potential for attacks, both in frequency and severity.

Belgium, as well as The Netherlands, find themselves competing with actors such as Russia, who have demonstrated their capabilities to disrupt our new crucial lines of communication² on and beneath the seabed. Whether related to energy, gas or telecommunications. A primary challenge in addressing this issue is the ownership of these cables, which are typically controlled by global business conglomerates rather than states, leading to complex ownership models. In response, Belgium has taken proactive measures by revising its legislation to protect its Critical Maritime Infrastructure (CMI). The latest revision is the New Maritime Security Law which strengthens the National Maritime Security Authority (NMSA). The question is then, within this reinforced NMSA, what role is the Belgian Navy expected to fulfil?

The National Maritime Security Authority

The complex threats to CMI forces the Belgian Navy and NMSA to collaborate closely. Understanding the navy's role requires first examining the NMSA's objectives, rooted in the New Maritime Security Law and EU directives, before focusing on the navy's operational contributions and resources within this structure.



Belgian minister of Defence Francken visits Belgian navy base at Zeebrugge, June 11th 2025 (source: BE Ministry of Defence)

Root directives

EU directives, notably the Critical Entities Resilience (CER)³ and the Second Network and Information Security (NIS2)⁴, shape the NMSA's goals, responding to attacks like Nord Stream by promoting cross-border resilience. The CER directive requires member states to strengthen essential services⁵ in energy, transport, and digital sectors against hybrid and climate risks. The NIS2 directive enhances cybersecurity for critical service operators, including protections for undersea communication cables. The EU Maritime Security Strategy (EUMSS)⁶ calls for better risk assessments, underwater CMI protection, counter-drone measures, and integration with renewable energy; roles assigned to the NMSA and our Ministry of Defence as key factor in safeguarding vital services.

New Maritime Security Law

The New Maritime Security Law⁷, in alignment with the EU directives, has been a major national initiative. Enacted on 1 January 2023, it extends the scope of the NMSA⁸, which focusses on ports and port facilities, to include CMI at sea. This law enhances the NMSA's responsibilities in approving safety assessments and plans for construction, civil engineering works, cables and pipelines. Currently, the NMSA is identifying Belgian critical entities, leading to a

comprehensive list of infrastructure, each with its risk assessment and mitigation measures.⁹ Special attention is given to more vulnerable points, like unburred pipelines and cable crossings. Those be monitored as areas of interest for the Maritiem Informatie Kruispunt (MIK) and Maritime Operation Centre (MOC). Sector-specific regulations are then issued by the Federal Service for Energy for gas pipelines and electricity underwater cables, and by the Belgian Institute for Postal Services and Telecommunications (BIPT) for communication cables. NMSA coordinates this sectorial approach, ensuring consistent and comprehensive regulations regarding the protection of CMI are being issued and correctly implemented.

**‘Seabed warfare
could be turned
into opportunities
for Belgium, Belgian
industry and knowledge
institutions’**

Proposed Resolution

After the new law was published, a proposed resolution has been issued at the Chamber of Representatives for a seabed strategy to protect Belgian interests.¹⁰ The division of responsibility could be a key factor in it, including clear statements about the role of the navy. It also states that with the right focus and investment policy, seabed warfare could be turned into opportunities for Belgium, Belgian industry and knowledge institutions. As a matter of fact, it already has relevant specializations and internationally recognized expertise in Mine Counter Measures (MCM). The navy will need to build further on this expertise to broaden capabilities to detect and eliminate any potential threat on the seabed that could affect the integrity of CMI. These include classic and smart mines, sabotage charges, the growing threat of unmanned and autonomous underwater vehicles and eavesdropping devices. The navy should therefore engage MCM Lab and ECA Robotics Belgium on CMI protection within the development of new MCM capabilities in coordination with and eventually sponsored by EU or NATO initiatives.

Furthermore, the resolution highlights the need for the navy to broaden its maritime domain awareness (MDA) especially below the water surface. This can be done by improving the knowledge of the underwater environment, increasing availability of the Patrol Vessels¹¹ and equip them with towed acoustic devices, use of drones, increased number of sensors on CMI and use of artificial intelligence at the MIK to analyse information. The coastguard structure is now 20 years old and needs to be updated to not only watch over the sea, but also in the water column and on the seabed. This should result into a single operational picture covering activities above and underwater and could lead to an automatic detection and identification system.

Ostend Declaration

On 24 April 2023, nine countries¹² met in Ostend for the North Sea Summit to establish a strategy to increase and connect the offshore capacity of wind energy production in the North Sea. The summit ended by the signature of the Ostend Declaration stating that participating countries will work together within NATO and the EU to increase the security of offshore and underwater infrastructure, to protect the common interests, uphold international law and react effectively to growing traditional and hybrid threats in the North Sea. The use of the NATO framework makes the navy an essential permanent member within the NMSA and therefore the navy is present in the CMI related forums at NATO and EU¹³. This substantial increase in offshore capacity means for the NMSA an increase of CMI to be assessed, regulated and protected. It also gives the opportunity to increase the number of underwater sensors in the North Sea by asking it in the mitigation measures before permits are being given. The navy can have an advisory role and create the link between the industries and the critical entities for the acquisition of sensors.

For the realization of the Princess Elisabeth energy island in front of our coast, as shown on Figure 1, minimum mitigation measures asked by the NMSA could be an acoustic shield (hydrophones), radars, docking stations and cameras. It would help the navy to improve her maritime awareness and ease interventions if needed. Those requirements will be at cost of the operator but the monitoring and, if needed, the interventions would be done by the partners of the Belgian coastguard including the navy. The islands will also be connected to the Danish Energy Island¹⁴ and therefore coordination with Denmark is needed regarding the measures to be taken by the operator.

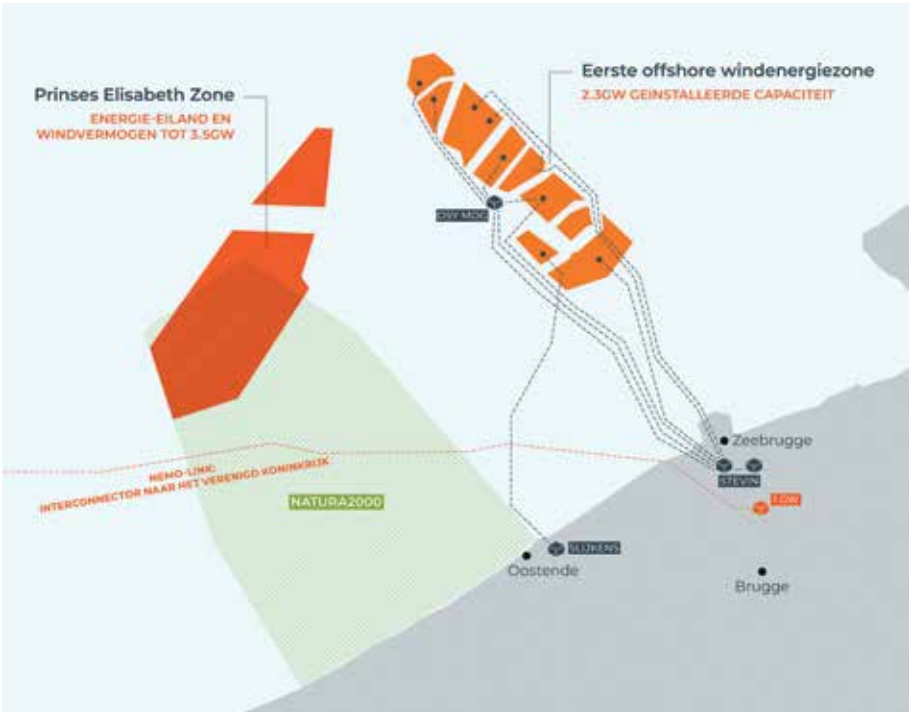


Figure 1: Princess Elisabeth Island (source: Industrie LINQS/Elia)

The New Maritime Security Law

Role of the navy within the National Maritime Security Authority

Mandatory role of the navy

The NMSA meets at least four times a year, is led by Directorate General Shipping and seats representatives from key departments, including the National Crisis Centre, State Security Service, Administration of Customs and Excise, Office for the Coordination of Threat Assessment, Navigation Police and Ministry of Defence with representatives from the General Intelligence and Security Service (GISS) and from the Defence Joint Staff (fulfilled by the navy). It gives opportunities for the navy to give her position on regulations and on level of protection of CMI. Day-to-day operations of the NMSA, managed by the Maritime Safety Unit (MSU) of DG Shipping, include monitoring security at CMI, ports and port facilities. Where necessary, NMSA makes improvements through legislation, directives and instructions. The navy's contribution is further expanded through its reservist officer working at the MSU and its involvement in the NATO Maritime Centre for the Security of Critical Undersea Infrastructure (NMCSCUI)¹⁵.

Within the North Sea countries, there is an initiative to establish (in a first phase) an encrypted web-based network for sharing information among all actors, military or not, about suspicious activities. On the military side of information sharing, NATO networks will be used instead of EU. These networks will be settled in the MIK, located in the naval base in Zeebrugge, who continuously monitors the security at sea and establish maritime awareness. The MIK is part of the Belgian coastguard that gathers 17 governmental institutions (both regional and federal)¹⁶. The MIK operators of the navy will make the link with the MOC and NATO. NATO will form the overarching security organization due to its intercontinental localization of CMI, but also because it has the means to intervene and it gives the UK (non-EU) a place at the table.

Belgian Defence Strategic Vision

In her strategic vision *Plan Star*¹⁷ then minister of Defence Ludvine Dedonder already points out the direction to follow regarding protection of CMI. This vision is fully aligned with the national, EU and NATO recommendations: the need for capacities to protect CMI¹⁸, improving interdepartmental situational awareness of the MIK by collaboration with allies and public sector like using the future offshore energy island for the installation of sensors, communication systems and docking stations for drones¹⁹ and the future connection of the MIK to the Common Information Sharing Environment (CISE)²⁰. In her business plan²¹, the navy will be committed to seabed warfare: 'The navy will provide our country with maritime capabilities capable of being deployed with short pre-warning in our Territorial Sea, our Economic Exclusive Zone (...) and to defend the vital interests of the nation and its allies at sea, in the water column, on the seabed and below.'

If providing sensors could be asked to CMI operators, the navy needs to provide options to enforce regulations and defend CMI against an actual threat.

'The navy needs to provide options to enforce regulations and defend critical maritime infrastructure against an actual threat'

How to achieve it

Achieving it starts with a correct monitoring. A cooperation is also being investigated with Flanders Marine Institute that has already deployed acoustic sensors on the seabed to listen to sea mammals which could also be used for to detect ships. DG Shipping is going to purchase a secured 5G network to cover the whole Belgian part of the North Sea to enable communication with drones that will cover blind spots in the northern part of our EEZ²² with video or radar imagery. It sends real time tracking information to the MIK. This could be part of another ongoing project. On the actual wind parks, a contract already allows the navy to have access to camera images of those installed offshore. But the main threat for these farms is assessed to be cyber.

The collected information then needs to be processed. To increase our maritime awareness, Artificial Intelligence and machine learning will be used in the near future on all received information to identify suspicious activities near areas of interests such as leisure crafts going at anchor or unusual fishing patterns. Based on threat assessment, NMSA can enforce additional areas where fishing activities will be prohibited (fishing vessels are occasionally used to gather intelligence by some nations). Temporarily forbidden areas to protect critical infrastructure are unacceptable for shipping activities. If protection is deemed necessary, to enforce an interdiction or investigate suspicious behaviours, as no other partner have assets to fulfil this task, it will be a task of the navy in coordination with other partners. For example, forcing an intruder outside a prohibited area could be a task for a patrol vessel.

Through collaborative dialogue with the defence Industry, the navy can explore and develop alternatives to patrol vessels, offering innovative and effective solutions. Seabed warfare was introduced at the European Defence Agency (EDA) in 2020. With the upcoming revision of its Capability Development Plan²³, EDA will develop interconnected capabilities and explore key technologies required to manage maritime unmanned drone swarms and to protect critical seabed infrastructure.²⁴ This could give indications for the Belgian defence industry and for minimum requirements of future CMI. Not only underwater drones will be needed for surveillance but also air drones. This would be the quickest way to investigate suspicious behaviour and collect data. With the replacement of the coastguard aircraft, the acquisition of drones should be considered as well.

Neutralizing the effectiveness of sabotage is an efficient deterrent strategy. Consequently, redundancy will be imposed for energy cables as a mitigation measure (also opted for the Princess Elizabeth energy island) whereas for pipelines this is unaffordable. Instead, the resilience of the Belgian pipeline network is fortified through a robust system of interconnections, an area where Belgium particularly excels²⁵. In the realm of communication cables, redundancy is already a standard practice. The network can reconfigure itself in milliseconds, switching to alternate cables if necessary. However, limitations remain. As depicted in figure 3, should seven key cables be severed, Belgium could face partial isolation from the global network, resulting in significant economic and societal impacts. To further mitigate risks, future cables will be buried deeper, enhancing their protection against potential threats.

When suspicious behaviour is detected, like a vessel stopping on top of CMI, an inspection of the CMI is needed. NMSA may therefore increase the frequency of seabed scans using side-scan sonar on civilian vessels, beyond the usual annual schedule. The navy could help identifying objects during those surveys and, if needed, neutralize it at later stage. The navy's new MCMVs, equipped with advanced toolboxes and underwater robotics, are ideal for this purpose, functioning effectively up to 300 meters deep.²⁶ For deeper CMI beyond the North Sea, Belgium's navy focuses on conventional anti-submarine warfare, relying on NATO and EU allies, like France²⁷ and the UK²⁸, who are developing capabilities for greater depths.

Challenges facing disruption

A physical intervention to protect the CMI might still be needed. Those measures can only be taken in strict compliance with the law. While such measures can easily be envisaged and implemented in the territorial sea, where the coastal state enjoys almost total sovereignty. It suffers limitations in the EEZ, where, as UNCLOS²⁹ stipulates, the coastal state's sovereign rights are more restricted. For example, Belgian jurisdictional powers do not extend to cables and pipelines located beyond the territorial sea, except for those 'installed or used in connection with the exploration of its continental shelf or the exploitation of its resources, or the exploitation of artificial islands, installations or structures under its jurisdiction'³⁰, and/or in the event of an incident resulting in environmental damage.³¹

The Belgian Maritime Code (2020) is setting up regulations within the limits of the sovereign rights. An adaptation of the international laws to protect all CMI outside the territorial sea is needed and is a priority of DG Shipping. A robust legislation has a deterring effect on potential aggressors. In the event of CMI disruption, our National Crisis Centre will take the lead in coordinating response efforts on land, while the navy is likely to lead operations at sea, providing resources and expertise on-site. Should there be any casualties or pollution, these incidents will be addressed through the activation of the national contingency plan, under the guidance of the Governor of West Flanders. The effectiveness of this coordinated approach also hinges on regular training that involves all partners.

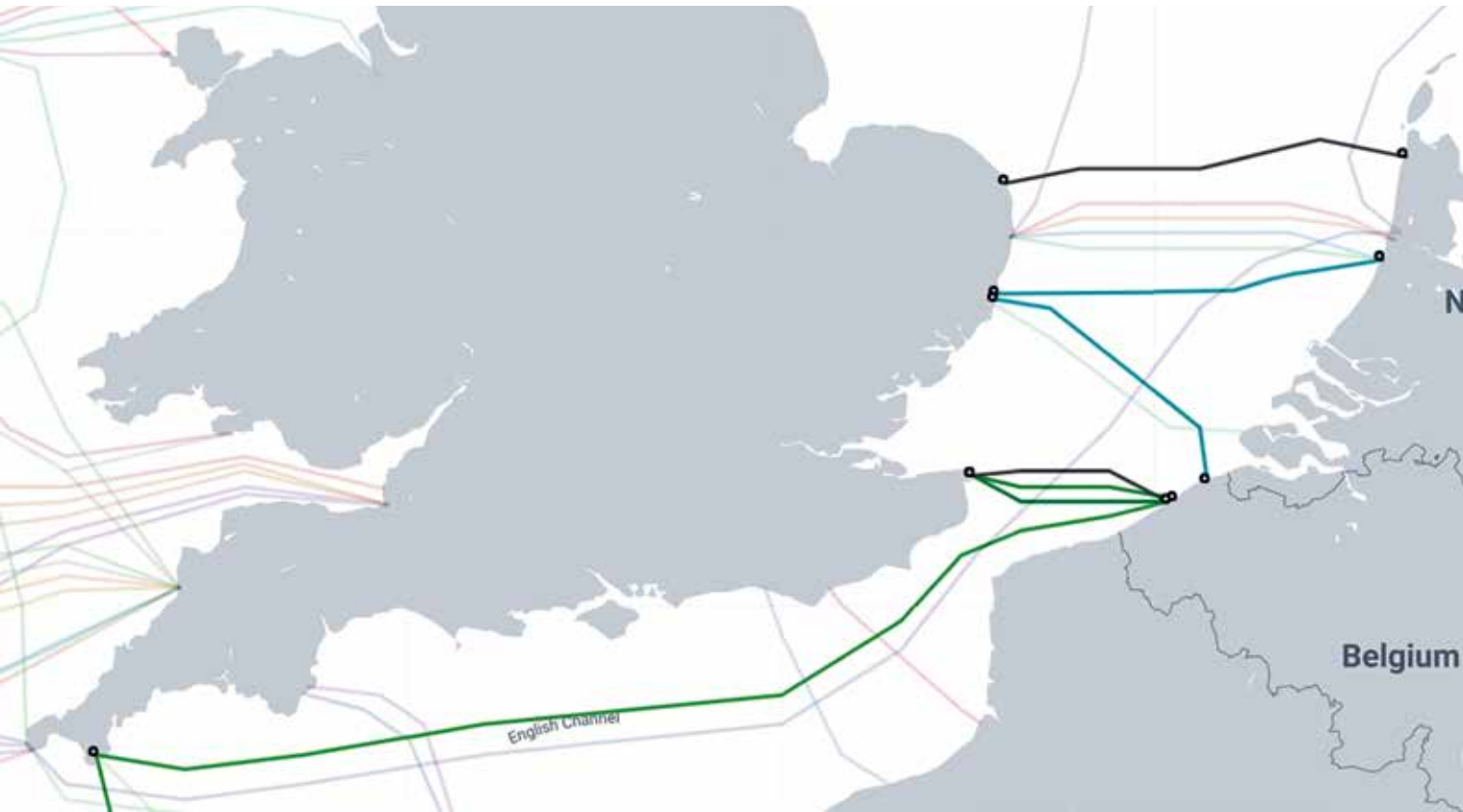


Figure 3: the seven vital communication cables of Belgium (source: submarinecablemap.com)



Repair drone for underwater infrastructure, Saab Sabertooth (source: SAAB)

The EU mandates annual training exercises: a standard Belgium has already met with exercises like COASTEX 2023. In the event of disruption, the resilience of CMI is crucial. Unfortunately, the availability of repair resources is notably limited. Gas pipeline repairs, for instance, can take from two months to two years, depending on the severity of the damage, weather conditions, and the availability of the three specialized EU repair ships.³² It may be prudent for the NMSA to advocate for investment in additional repair vessels as part of the EUMSS. While repair ships for communication cables are more accessible, their repairs could still require up to six weeks. Another challenge for the resilience is the scarcity of spare parts. Operators might consider this in their security plans, including expedited repair methods such as drones as a mitigative measure. Considering these challenges, particularly in the context of repair capabilities and the use of advanced technologies like drones, the Belgian navy's participation in the EU Critical Seabed Infrastructure Protection (CSIP) project under PESCO becomes increasingly relevant.³³ This involvement would not only leverage the navy's expertise in mine and seabed warfare but also ensure its awareness of the latest technological advancements. Such a move would be perfectly aligned with the Defence, Industry, and Research Strategy³⁴.

At last, a development of Offensive Seabed Warfare capability able to target a potential enemy's CMI should be considered as an effective mean of conventional deterrence. The capability would include information gathering on CMI and could also be part of our future mining capacity or special operations technics. This would need further reflection on the wanted and consecutive effects of such attacks.

‘While repair ships for communication cables are more accessible, their repairs could still require up to six weeks’

Conclusions

Our modern Sea Lines of Communications, running on the seabed through cables and pipelines, are put at risk within the current geopolitical situation and the growing accessibility of technologies like underwater drones. The new Maritime Security Law provides an enhanced legal framework to protect them and, among other things, reinforces the role of the NMSA. The navy is and will remain a key permanent member within the NMSA taking part in the decision-making process, providing guidance on securing CMI, and helping with risk assessments.

Through NMSA risk assessment of critical entities, operators can be forced to provide enough sensors to detect threats to their CMI and increase their resilience. This will improve the MDA of the navy and set the most favourable conditions for when the MIK will task its Coastal Security and Harbour Protection capability on a real threat. The security of CMI requests innovative technologies that must be developed in dialogue with civilian operators, defence industry and within the framework of NATO, EU or bilateral cooperation. To effectively fulfil its responsibilities within the NMSA, the navy needs to sustain expertise within the Defence Staff and actively participate in NATO and EU forums focused on CMI. This expertise is cultivated not only through reserve officers but also within its specialized Coastal Security and Harbour Protection units.

After a full career in operations, Commander GS Gaëtan Motmans (Belgian Navy) was appointed head of the Maritime Operations department at the Defence College in Brussels, where he teaches at the Advanced Staff Course.

SCAN DE QR-CODE
VOOR DE VOETNOTEN
BIJ DIT ARTIKEL

