



# *“The underwater and deep sea domain: emerging threats and opportunities for NATO powers”*

di Angelica Gimbo

COMMENTO CESMAR NR. 30 – gennaio 2025



<https://iadnews.in/need-for-underwater-domain-awareness-uda/>

CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



## **Index**

<b>Introduction</b> .....	<b>2</b>
<b>Chapter I</b>	
<i>The maritime space and its critical infrastructures</i> .....	<b>3</b>
<b>Chapter II</b>	
<i>The NATO Strategic Concept: its evolution over the years. A focus on the 2022 NATO SC</i> .....	<b>5</b>
<b>Chapter III</b>	
<i>The underwater and deep sea dimension as a new NATO domain: strategic threats and opportunities</i> .....	<b>8</b>
<b>Chapter IV</b>	
<i>Governance and international responsibility in the underwater domain</i> .....	<b>10</b>
<b>Final remarks</b> .....	<b>13</b>
<b>Bibliography</b> .....	<b>15</b>

### **Introduction**

Earth's surface is covered by sea waters for 70%. Namely, under this percentage there lies every resource, supply, and capacity that the humankind needs to survive by leading a life above the waters. Still, 80% of the seabed and 97% of the oceanic abyssal depths remain unexplored, notwithstanding the universal recognition of the underwater sea domain as one of the most significant strategic environment for the benefit of economic and geopolitical development, as well as of energetic, mineral and even digital resources' exploration towards our communities.

Against this backdrop, it could be argued that over successive generations we have come to be better acknowledged on the specifics regarding the surface of the Moon, or planets as Mars and Jupiter, than on the seafloor environment itself. This instance displays the result of 'space' being recognised as a new strategic warfare domain, playing a critical role in transmission, supervision, navigation and information sharing capacities, and stemming as a deciding element of NATO's future defence stance. Just in 2021, 370 billions of dollars have been invested in the space domain and a 73% increase is envisioned to be implemented in a ten-years timeframe.<sup>1</sup> Conversely, with reference to the underwater sea domain, it has been foreseen an investment rise from the

---

<sup>1</sup> Euroconsult Annual Space Economy report (2022), [Space Economy Report 2022 - Euroconsult's Digital Platform, euroconsult-ec.com, https://digital-platform.euroconsult-ec.com.](https://digital-platform.euroconsult-ec.com)

CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



current earmarked three billions of dollars up to twelve billions to be reached in 2033 only for drones acquisition.<sup>2</sup>

Considering that nowadays digital communications sweeping through space satellites account only for the 2-3%, compared with the 98% of underwater information transit traversing through underwater cables (mounting up to one trillion of undersea cables transactions only in 2022<sup>3</sup>), it appears imperative to define the underwater domain as the sixth NATO military domain, in addition to the already recognised air, sea, land, cyber and space ones.

Indeed, for decades navigation safety and security have historically been focused almost entirely on maritime activities conducted by surface vessels, while submarine deployment remained a domain reserved exclusively for the military sector. Despite this long-standing dichotomy, maritime security is now engaging further actors and concerns, given the underwater-related emerged implications.

## Chapter I

### The maritime space and its critical infrastructures

The maritime space appears as a multi-layered, three-dimensional area whose infrastructures not only are on the sea, in the sea, and on the sea and ocean floor, but they also overpass and intertwine each of these scales. Currently, 90% of global transportation is attested to be seaborne as a consequence of the transformative headway that involved loads of ocean-based activities to the point that we moved from shipping lanes, telegraphic cables and ports as critical infrastructures to a current reliable extended set of sea infrastructures. Tankers, pipelines, gasifiers, windfarms, ports, subsea electricity and fiber data cables, landing stations, cable repair vessels are only a few of the vast examples of contemporary “critical maritime infrastructures”, which shipping industries, economies and societies are now fully dependent from.

The concept itself of critical infrastructure emerged quite late during the 1990s and consequently spurred new security debates around the policies that would have been needed to ensure its protection. Given that the ocean floor accommodates 487 undersea cables accounting for 1,3 millions of kilometers<sup>4</sup>, the foundation of digital communication and electricity makes trade and supply chains, energy and food security utterly interdependent one to the other and reliant on them, posing critical maritime infrastructures and their security at the core of national and international maritime security agendas.

Usually, the kind of maritime infrastructures to which is given most of the attention are those falling within these categories: shipping, energy, communication through optic fibre cables, fishing, and marine biodiversity. Their components are a perfect example of the interdependence that maritime critical infrastructures are exposed to as critical nodal points, as for the case of the Port of Marseille, which functions as a pivotal transportation maritime hub, and at the same time houses cable landing stations and its cable repair vessels for maintaining energy supplies and ensuring data flows. An additional instance to be considered within this frame may be the cases of the Red Sea or the Strait of Malacca,

---

<sup>2</sup> Center for International Maritime Security (CIMSEC), <https://cimsec.org/>.

<sup>3</sup> Signifying an estimated value of 10 trillions of dollars and a 12% of annual growth rate, according to TeleGeography society, <https://www2.telegeography.com/en/our-research>.

<sup>4</sup> Source: <https://www.thewatcherpost.it/economia/geopolitica-dei-cavi-sottomarini-il-convegno/#:~:text=Ben%20487%20sono%20i%20cavi,mondo%20se%20ne%20contano%20109>; <https://www.geopop.it/cavi-sottomarini-dove-passa-la-fibra-ottica-dei-nostri-dati-altro-che-satelliti/> (last accessed on: 10/01/25).

#### CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



which represent essential maritime transport chokepoints, and the main routes for data cables by bridging the European and the Asian continents, as they happen to be two of the world busiest waterways for international trade, hence located in a hyperdense concentration area of maritime infrastructures.

One last example that shows either that sea interconnectivity has been recognised as the most effective and efficient transportation mode, and that poses several threats and challenges that need to be paid attention to and tackled by tailored maritime security policies is the 2022 attack on the Nord Stream pipelines located in the Baltic Sea, specifically between the EEZs<sup>5</sup> of Sweden and Denmark: this type of incidents, whose responsibility in the majority of cases has still not been attributed to any State nor individual, exemplifies the need for a shared maritime governance to draft an overarching set of rules that would be able to ascribe responsibility to emerging acts of terrorism, blue crimes, grey zone tactics or any other potential threat against maritime infrastructures. Critical maritime infrastructures need to be shielded by protective recourses, be brought to the forefront of public discourse and turned into a top political priority at both national and international level. That's the reason why the Allied countries decided to address the underwater dimension as a focal point of NATO's security concerns and frame it within one of the core elements of its defence strategy, namely, the maritime domain.

As new challenges in the maritime domain have arisen thanks to the progressive technological advancements, as submarine warfare and autonomous underwater vehicles (AUV), major attention has been devoted to the increased militarization of underwater warfare, including threats to undersea cables. A protection system aimed to uphold freedom of navigation, secure maritime trade routes, protect LOCs<sup>6</sup>, and safeguard critical infrastructures as energy pipelines from sabotage, non-conventional attacks, or technological warfare is considered to be necessary to be put in place, since maritime security is acknowledged as a key to Allies' peace and prosperity.

The 2022 NATO Strategic Concept envisaged in Madrid refers to these needs by underlining the strengthening of NATO's defensive posture and the reinforcement of maritime situational awareness, in order to keep deterring against newly emerged maritime and undersea threats.

## Chapter II

### **The NATO Strategic Concept: its evolution over the years. A focus on the 2022 NATO SC**

The NATO Strategic Concept (SC) outlines the Alliance's main purposes and strategic priorities addressing unfolding threats, challenges and opportunities. This document results to be the final output of a regular and progressive reworking in accordance with the systematic evolution of the geopolitical scenery and the actors involved. The first Strategic Concept, "the Original" one, was adopted in April 1949 at the signing moment of the North Atlantic Treaty itself and constituted the founding concept of the Alliance, originally based on the pivotal concepts of deterrence and collective defence<sup>7</sup> against the threat posed by former Soviet Union's enlargement and the potential spread of communist regimes across western Europe. One of the key elements to be outlined in the original Concept is the consideration devoted to the resort to conventional forces that, following the emergence of new war domains that extend beyond traditional battlefields, will be later overcome. Indeed, already with the 1957 SC, the concept of deterrence was further integrated with the unconventional nuclear type of defence, since the balance of power

---

<sup>5</sup> EEZ(s) stands for Exclusive Economic Zone(s).

<sup>6</sup> LOC stands for Lines Of Communication.

<sup>7</sup> Art.5, NATO Treaty, [https://www.nato.int/cps/ie/natohq/topics\\_110496.htm](https://www.nato.int/cps/ie/natohq/topics_110496.htm).

#### CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



among NATO Allies and their counterparts grouped in the Warsaw Pact started to depend on nuclear weapons' growing capacities and its ensuing deterrence. Ten years later, with the Cold War season fully underway, by acknowledging the status of nuclear parity between the United States (US) and the former Soviet Union, the 1967 SC chose to adopt the *détente* policy among the superpowers: the document oriented NATO's defensive posture towards strategic stability rather than overwhelming supremacy. This effort signalled the enduring reliance on nuclear deterrence while combining a more flexible strategic response to both conventional and non conventional forms of threats.<sup>8</sup> Conversely, the 1991 SC marked a shift in what it was outlined as a purely defensive NATO stance: since the end of the Cold War, the dissolution of the Soviet Union, and the resulting NATO's first rounds of enlargement into Central and Eastern Europe generated a post-Cold War environment qualified by crisis management, cooperative security towards emerging democratic nations, and cooperation with former adversaries.<sup>9</sup> In line with this transformative defence posture, the 1999 SC, adopted during the Washington Summit, outlines a global environment whose actors no longer had as top priority contending with the communist expansion threat, but rather to deal with, and later prevent, the instability driven by new regional conflicts and spread out humanitarian crises by engaging in out-of-area operations. Along with this purpose, the springing up of a multipolar world prompted NATO members to keep on fostering further forms of cooperation and partnerships with international organisations and non-Allied countries to deal with new security threats. Accordingly, the 2010 SC, adopted at the Lisbon Summit, acknowledged the need to address non-traditional security threats as terrorism or cyber attacks as game-changing challenges against which a more militarily effective and adaptable force should have been put in place through a smarter collaborative use of resources. Finally, the latest and most recent SC, adopted at the 2022 Madrid Summit, depicts NATO's gained awareness and complete recognition of the swelling multiplicity of current warfare: new war domains mirror just-out global security issues that comprise both military forces and state-based threats, and multi-domain, hybrid, asymmetric type of warfare.

On this matter, Russian Federation's invasion of Ukrainian territory in February 2022, carried out also through hybrid tactics, marked out a striking shift in global security concerns, leading NATO for the first time to point out the Russian Federation as the most significant and direct security threat; on the other hand, China is not yet referred as an adversary, but as an "emerging challenge" whose soft power and global influence in technology, infrastructure, and military expansion need to be addressed. Moreover, cybersecurity threats, climate change, terrorism, non-state actors, space, new technologies, artificial intelligence and autonomous systems, great power competition, and hybrid warfare tactics are identified as the latest sprout drivers of security risks in exacerbating tensions, that may lead to augment the likelihood of conflicts which may spur across the globe.

In order to tackle conventional and hybrid threats, 2022 NATO SC's answer comprises the following elements: nuclear deterrence to ensure strategic stability; resilience and adaptation addressing a wide range of non conventional challenges and the protection of critical systems against disruption; global partnerships strengthening loyal rings; more robust military and political alliances' commitment to modernize command structures and defence-industry capacities to respond quickly to crises.

Still, the latest SC acknowledges a frame within which the following war domains are likely to become modern warfare's areas of focus for NATO in the future: cyber domain against cyber attacks and digital warfare; space domain

---

<sup>8</sup> The flexible response strategy was inspired by the threat of Mutual Assured Destruction posed by Cold War opponents to nuclear weapons' race.

<sup>9</sup> For instance, as through Partnership for Peace programs.

#### CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



as for space-based assets protection, missile defence, satellite systems, anti-satellite weapons (ASAT)<sup>10</sup>; hybrid warfare as for information, propaganda, psychological and cognitive warfare (and even economic pressure through sanctions and trade restrictions); electromagnetic spectrum (EMS) domain as for the use of electromagnetic interferences to disrupt military operations and communications; climate change domain and environmental weaponization as for weather modification and resource shortages; biological warfare as for synthetic biology misused to destabilize, against which biosecurity is being developed; and the underwater and deep sea domain as for submarine warfare's increased militarization (to which the following chapter will be entirely devoted).

### Chapter III

#### The underwater and deep sea dimension as a new NATO domain: strategic threats and opportunities

As underscored in the previous chapter, NATO powers are exploring possible ways of adaptation of their military capacities to coherently address the emerged warfare challenges in a multi-domain security environment, which clambered up to be the top priorities of contemporary NATO defence policies' agenda.

One of the most significant domain that is likely to reshape the nature of future conflicts, due to the growing dependence on underwater and oceanic-based critical infrastructures, is constituted by the underwater and deep sea domain, on which this chapter will be focused.

Albeit the maritime domain has always belonged to NATO's defence strategy as one of the core elements in terms of naval surface warfare, the underwater and deep sea domain is currently turning into a critical point of NATO defence strategy, since it involved security concerns regarding an entirely new warfare category: as stated in the 2022 NATO SC itself, attacks or sabotage episodes against critical maritime infrastructures as underwater cables and energy pipelines, cyber-physical systems like the Internet of Underwater Things (IoUT)<sup>11</sup>, as well as the competitive race over undersea rare resources' control, are likely to constitute an additional vulnerability for States' security.

As it was described in the first chapter, underwater cables are the backbone of global communications and internet infrastructures, withstanding almost the entirety of international data traffic; therefore, their disruption would signify devastating strategic consequences on global security. Undersea pipelines, carrying energy supplies around the globe, are further examples of vulnerable infrastructures that could turn into strategic military targets, whose protection must be ensured by resorting to patrolling underwater drones, defence-aimed private-public joint operations, or other surveillance tools to be used as countermeasures.

Additional threats posed within the undersea domain refer to the following risks: the strategic control of the deep-sea mining industry in disputed waters over deep-sea marine resources, as gas, oil, cobalt, and other rare seabed minerals, and the ensuing environmental impact on marine protected ecosystems induced by climate change-driven resource competition<sup>12</sup>, which are likely to lead to rapid conflict escalation; the risk of underwater operations in case

---

<sup>10</sup> NATO's new Space Policy emphasizes the need for improved space situational awareness and the development of defensive and deterrent capabilities in space, <https://www.act.nato.int/our-work/network-community/natos-approach-to-space/>.

<sup>11</sup> The IoUT refers to the network of connected devices in the ocean: sensors, monitoring stations, underwater vehicles.

<sup>12</sup> Especially in the Arctic, as melting sea ice grants alternative shipping routes, increasing the likelihood of conflict over resource access.

#### CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



of use of sonar systems in anti-submarine warfare; terrorism-related covert underwater operations using scuba gears, manned submersibles or even underwater explosive devices. Furthermore, both nuclear-powered, ballistic missile, conventional, and attack submarines remain pivotal in intelligence gathering and those covert operations framed by naval deterrence strategy policies, since they were assembled to remain hidden and undetected underwater, hence less vulnerable; as a result, the anti-submarine warfare capabilities, comprising underwater drones and sonar systems, evolved into an obligation for NATO powers to counter underwater threats as AUVs, quiet propulsion systems, or other stealth, unmanned, counter-detection systems.

The 2022 NATO SC indeed, refers to the urgency of equipping Allied powers with appropriate monitoring systems to defend undersea infrastructures and secure underwater communication lines, by setting up cable protection teams, cybersecurity measures as surveillance drones, sensor networks and unmanned underwater vehicles, and by setting up joint defence forms of collaboration with civil private companies and research institutions engaged in subsea exploration activities, in order to enhance the maritime domain awareness. Additionally, the strategic document outlines a proactive environmental strategy in levelling off the marine ecosystems' damages induced by military activities on one hand, and the universally shared sustainability requirements towards the protection of the maritime environment on the other. The impressive technological headway that is underway in the field of undersea operations proves that maritime robotics like robotic maintenance platforms and swarm drones are effective answers to underwater repair and exploration issues that would not resort to human intervention, remarkably lowering the associated risks. It follows that the underwater domain mirrors the interrelation between the different ways of conducting modern warfare, whose conventional military capabilities are supplemented, sometimes even replaced, by hybrid, asymmetric, transnational tools. Integrated strategies addressing both the challenges and threats of this new domain are being developed and adapted to make NATO ensure regional security.

Against this backdrop, the undersea area of military strategy outlined as a future NATO military domain, enclosing underwater maritime security, infrastructure defence, submarine warfare, is likely to turn into a nodal sphere for the forthcoming international defence and deterrence strategies.

Beyond the mentioned threats to which NATO powers will have to stand up, the undersea domain also offers notable strategic opportunities that are worth being acknowledged. From generating economic interests in both military and civilian technological industries, to ensure strategic partnerships and regional alliances among coastal nations, non-member States, emerging powers, and private entities; from signing environmental agreements on seabed resource sharing and offshore underwater manufacturing and production, to secure underwater transportation routes, supply chains, and logistic lines.

As a result, as a further NATO domain-to-be, the underwater and deep sea focus area is plausible to turn up as a complex and multifaceted arena encompassing strategic opportunities in terms of deterrence advantages, capacity access, geopolitical leverage, and industrial leadership, by investing in sustainable practices aimed at securing what lays underneath the sea.

## **Chapter IV**

### **Governance and international responsibility in the underwater domain**

One of the main issues of the underwater and deep sea domain definitely lies on the criticality of knowing who and what is moving underneath sea waters and which are its objectives, aims,

CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



intentions. This is the reason why it has become a focal matter in the international law system and geopolitical affairs.

At present, the regulation over undersea activities and actors is structured within a complex, lacking and parceled governance framework, which involves international laws, regional agreements, national policies, only up to a forty-meters depth maximum from water surface, leaving the standardization of what rests beneath to be unregulated and likely to be targeted without any jurisdictional attribution.

Indeed, international regulation is conditioned by the coastline geography and the geology of the continental shelf: since the utmost depth for a country's exclusive rights reaches up to 350 nautical miles (nm), the applied legal framework here is UNCLOS<sup>13</sup>, which regulates seabed activities up to the continental shelf; on the other hand, since underwater areas exceed national laws' gauge of thousands of meters, the deep sea areas are regulated by the International Seabed Authority (ISA). It follows that the underwater domain is governed up to the limits of national jurisdictions of each State, while the waters falling out of these demarcations are governed by overarching governance bodies.

UNCLOS is the ultimate comprehensive international treaty regarding the management of global oceans and seabed activities. It was adopted in 1982 and entered into force in 1994 with the aim to rule over the underwater areas up to a specific depth, depending on the activities performed: territorial seas up to 12 nm benefit from full sovereignty rights over seafloor and water columns; in the EEZs, sovereign rights are recognised only on subsoil resources and not over the water column up to 200 nm, but cable laying and extraction activities are run from coastal States; seabed resources' exploration rights are also regulated by the Convention<sup>14</sup> but only up to 350 nm.

UNCLOS encompasses freedom of navigation for all States in international waters, environmental protection to preserve marine biodiversity, and marine scientific research to face transboundary environment threats which may emerge. ISA instead, is an autonomous international organisation set up in 1994<sup>15</sup> under the provisions of Part XI of UNCLOS and it frames the rules for the resources located in international seabed areas, considered as common heritage for the whole humanity; it oversees deep seabed resources' exploitation, and it gets applied to all the cases beyond national jurisdiction.

The underwater-related governance framework also comprises the following tools: the IMO<sup>16</sup> that ensures global standards for international shipping's security; regional agreements and bodies as the RFMOs<sup>17</sup> managing fishery resources; environmental agreements as the Barcelona Convention<sup>18</sup>;

---

<sup>13</sup> UNCLOS stands for the United Nations Convention on the Law of the Sea.

<sup>14</sup> Here is referred to the beforementioned UNCLOS.

<sup>15</sup> It became operational in 1996.

<sup>16</sup> IMO stands for International Maritime Organisation.

<sup>17</sup> RFMO(s) stands for Regional Fisheries Management Organizations.

<sup>18</sup> The Barcelona Convention refers to the "Convention for the Protection of the Mediterranean Sea **Against Pollution**", adopted in **1976** and entered into force in **1978**. It is a regional international agreement aimed at reducing pollution in the Mediterranean Sea.

#### CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



regional sea conventions, and country laws including national security laws on maritime traffic and infrastructures.

Additionally, in order to reinforce undersea infrastructures' security, governments and international stakeholders released a Joint Statement<sup>19</sup> on the occasion of a New York-based event of the UNGA<sup>20</sup>, that was later upheld by the European Union to confirm the shared effort towards strengthening seafloor cables' resilience and providing security from emerging threats. It recalls the international community's proactive cooperation to safeguard interconnected States in a globalized world.

Notwithstanding the just outlined legal framework which is currently responsible for governing underwater domain and seabed-related activities, it appears clear that, as the undersea domain turns into a more contested and interests-attractive area, a future set of rules will be needed to face new threats and mitigate rising tensions. Devising modern codes of conduct and rules of engagement for military underwater operations, as well as binding agreements or treaties revisions on sustainable extraction practices within a multilateral framework will be necessary to avoid a critical overlapping between undersea resource competition and interstate rivalries. Moreover, cybersecurity protocols for seabed infrastructures should be envisioned against sabotage or other type of attacks from unknown offenders. Expanding the scope of already existing conventions and drafting entirely cutting-edge environmental treaties should be a priority for the international community to govern human-induced performances in deep sea areas. For instance, expanding the mandate of the ISA beyond the limit of mining activities in resource management related to marine genetic, energy, and biotechnology capacities, and letting it rule over the environment supervision of deep-sea mining and oil drilling in international waters may be fruitful for the whole international community. A supplementary effort could be acted on by singular States enforcing tailored laws against seafloor cable damages, negotiating with cable owners to protect it as pivotal asset.

### Final remarks

As the complexity and the intersection of current strategic challenges affect the underwater and deep sea domain on a daily basis, it could be argued that an overriding body, may it be a global ocean governance entity, an interstate forum, or a newfangled multilateral treaty, might be established in the midst of a NATO framework.

It has to be acknowledged that, despite the existing governance frameworks act as a rooted groundwork, NATO powers must equip themselves with evolving governance structures to address the threats analysed, by advancing responsibility tools both at a regional and global level. This would be possible by demanding a multilateral integrated approach based on collaborative partnerships involving member and non-member States, industries, universities, stakeholders, research institutions, international organisations, and private companies through PPPs<sup>21</sup>. More than that, in order to ensure a peaceful use of the oceanic zones, establishing military demilitarized zones or buffer zones could be an alternative answer to protect seabed resources; regulating military exercises or submarine movements (and its actors) in geopolitically sensitive regions would represent an auxiliary governance model for the undersea

---

<sup>19</sup> The New York "Joint Statement on the security and resilience of undersea cables in a globally digitalized world" is a 2022 declaration aimed at pinpoint the relevance of undersea cables for global connectivity, issued by a group of nations, among which: the **United States, the United Kingdom, Australia, Japan, India, Canada**, some **EU members**.

<sup>20</sup> UNGA stands for the United Nations General Assembly.

<sup>21</sup> Public-Private Partnerships.

### CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.



domain. Finally, expanding on underwater exploration and data collection technologies may lead to good practices of monitoring, without jeopardizing the marine environment for the generations ahead.

One proposal that was recently laid out on this regard came from Italy, which at the end of summer 2024 put forward a draft law aimed at defining a suitable juridical frame to address the unbroken anthropization of the underwater environment. The proposed “Agency for the security of underwater activities”<sup>22</sup> aspires to be one of the first EU national law examples to set up firm rules regarding underwater traffic of activities and movements, as exemplified by the rule on the inoffensive passage of immersed submarines in Italian territorial waters, and by the attempt to draw up minimum security standards for the conduct of any underwater vehicle and its rescue in case of need. It has to be stated that, while Italy surely is a relevant actor in underwater heritage preservation and marine guardianship, it is not the first nor the pioneer NATO power to rule over the deep sea domain.

Drawing from these reasonings and taking into account the substantial investments in the maritime space’s surveillance and defence aimed at enhancing underwater security, it may be argued that maritime and deep sea domains’ awareness needs to be augmented to identify distrusting non-conventional threats, issue early warnings, rise the speed of incident responses, in order to prevent and counter them. Looking ahead to future generations, as more nations will militarily broaden their actions in underwater arenas, there remains the hope that by making the deep sea area an official NATO domain, the Allied powers will be able to pilot and steer legal controversies over maritime perimeters and undersea resource competition.

## Bibliography

---

- Bueger C., Liebetrau, T. *Critical Maritime Infrastructure Protection: What’s the Trouble?*, in *Marine Policy*, Vol. 155 (September 2023), Article 105772, (<https://doi.org/10.1016/j.marpol.2023.105772>, last accessed on 4/01/25);
- *Civilization of the Sea. The underwater world as a new environment for mankind: a conference promoting knowledge of the maritime dimension*, 22/03/23 ([https://www.leonardo.com/en/news-and-stories-detail/-/detail/leonardo\\_civilisation\\_of\\_the\\_sea](https://www.leonardo.com/en/news-and-stories-detail/-/detail/leonardo_civilisation_of_the_sea), last accessed on 5/01/25);
- *The underwater domain: the new global race is played out in the ocean depths*, Lightbox, 9/07/24, (<https://lightbox.terna.it/en/transition/underwater>, last accessed on 2/01/25);
- Calcagno, E., Marrone, A. *The Underwater Environment and Europe’s Defence and Security: the Italian approach to the underwater domain*. Published by: Istituto Affari Internazionali (IAI) (2023), (<https://www.jstor.org/stable/resrep51668.9> (<https://www.cesi-italia.org/en/articles/the-underwater-almost-domain-dependencies-threats-and-prospects-for-protecting-operating-and-excelling-in-the-abyss>), last accessed on 6/01/25);
- *Joint statement on the security and resilience of undersea cables in a globally digitalized world*. Media note, Office of the spokesperson, 26/09/24, (<https://www.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/>, last accessed on 7/01/25);

---

<sup>22</sup> “Agenzia per la Sicurezza delle Attività Subacquee”, ASAS, proposed within the draft law of Minister Nello Musumeci, comprised in the “Piano Nazionale del Mare”, that would be depending on the Italian Presidency of the Council of ministers, chaired by Giorgia Meloni at the time of writing.



- Das, A. *The Underwater Domain Awareness Framework: Infinite Possibilities in the New Global Era*, India Foundation (<https://indiafoundation.in/articles-and-commentaries/the-underwater-domain-awareness-framework-infinite-possibilities-in-the-new-global-era/>, last accessed on 7/01/25);
- Bueger, C., Liebetrau, T., Franken, J. *Security threats to undersea communications cables and infrastructure: consequences for the EU*. Policy Department for External Relations Directorate General for External Policies of the Union. PE 702.557, June 2022, ([https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO\\_IDA\(2022\)702557\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf), last accessed on 7/01/25);
- NATO *Strategic Concept*, June 2022, <https://www.nato.int/strategic-concept/>;
- Kaushal, S. *Stalking the Seabed: How Russia Targets Critical Underwater Infrastructures*, in *RUSI Commentaries*, 25/05/23, (<https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure>, last accessed on 1/01/25),
- Lesti, S., Zacchei, A. *La sicurezza marittima e le infrastrutture critiche subacquee. Un approfondimento degli scenari geopolitici, degli attori, delle minacce e delle tecnologie esistenti*. MInter Group, 2023, p. 23;
- Giannoulis, G. *Handbook on Maritime Hybrid Threats: 15 Scenarios and Legal Scans*, in *Hybrid CoE Papers*, No. 16 (March 2023), (<https://www.hybridcoe.fi/publications/hybrid-coe-paper-16-handbook-on-maritime-hybrid-threats-15-scenarios-and-legal-scans>, last accessed on 4/01/2025);
- Kotman, T. *Maritime Hybrid Threat*, Research Article, Navy Captain Support Branch Head, (<https://www.marseccoe.org/wpcontent/uploads/2021/08/Maritime-Hybrid-Threat.pdf>, last accessed on 8/01/25);
- Benedict, J. R. *Future Undersea Warfare Perspectives*. *John Hopkins Apl Technical Digest*, 21(2), April 2000;
- McNamara, E.M. *Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure*, *NATO Review*, 28/08/24;
- Bergeron, J. H. *From Maritime Security to Sea Power: Nato's Paradigm Shift*. ISPI, Italian Institute for International Political studies, 11/06/24, (<https://www.ispionline.it/en/publication/from-maritime-security-to-sea-power-natos-paradigm-shift-176619>, last accessed on 5/01/25);
- Detsch, J., Johnson, K. *NATO Wants to Boost Its Undersea Defenses. Officials fear Russia could cut the undersea cable network that undergirds much of the global economy*. *Foreign Policy*, June 2024 (<https://foreignpolicy.com/2024/06/24/nato-undersea-cable-network-russia-infrastructure-defense/>, last accessed on 5/01/25);
- Bukowski, M. *Underwater connections are vulnerable, the alliance lack a strategy to defend them*, 16/08/24;
- Cassetta, M. *How to Respond to the Emerging Threats to Critical Underwater Infrastructure at the Time of Russia's War Against Ukraine*. Rome, IAI, June 2024, 4 p. *IAI Commentaries*, ISSUE.

---

#### CESMAR – Commento

I contributi sono diretta responsabilità degli autori e ne rispecchiano le idee personali. Le foto presenti in questo commento sono state di massima prese dal web, citandone sempre la fonte. Se qualcuno dovesse ritenere necessario rimuoverle o modificarne gli autori, può contattarci sul sito [cesmar.it](http://cesmar.it) e sarà prontamente accontentato. La riproduzione, totale o parziale, è autorizzata a condizione di citare la fonte.