Istituto Affari Internazionali

ISSN 2532-6570

IAI COMMENTARIES 24 | 31 - JUNE 2024

How to Respond to the Emerging Threats to Critical Underwater Infrastructure at the Time of Russia's War Against Ukraine

by Marco Cassetta

Recent Russian assertiveness and the ongoing war in Ukraine have radically altered the threat perception in Europe, marking a turning point in the way current wars are fought. While NATO countries remain focused on supporting Ukraine and strengthening the Alliance's eastern flank, the Mediterranean Sea increasingly appears to be a highly unstable, uncertain and disputed environment, showing vulnerabilities that will not be easily resolved, especially in the underwater dimension.

The sabotage of the Nord Stream pipeline in September 2022 has forced European governments to face their limited ability to defend against hybrid tactics in the underwater environment.[1] Moreover, at the moment, it is not yet possible to ascertain whether the subsequent damage to the "Baltic connector" pipeline and a data cable between Finland and Estonia in October 2023 was in fact intentional or happened by accident.[2]

A new trend in warfighting and security

The intricate context of underwater critical infrastructures seems to be the perfect scenario for the conduct of malicious actions by using conventional assets, special forces, hybrid warfare or, in the case of non-state actors, terrorist attacks.[3] In particular, hybrid warfare tactics aim to cause significant damage by acting below the detection threshold, in the blurred boundaries between competition, crisis and high-intensity engagements.

[1] Sean Monaghan, "Five Steps NATO Should Take after the Nord Stream Pipeline Attack", in *CSIS Commentaries*, 6 October 2022, https://www.csis.org/node/67165.

[2] Richard Milne, "Finland Investigates Potential Sabotage to Baltic Gas Pipeline", in *Financial Times*, 10 October 2023, https://www.ft.com/content/8d9baf58-22c2-4456-905c-15fd7f9dcd69.

[3] Christian Bueger and Tobias Liebetrau, "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.

Marco Cassetta has Master's Degrees in Strategic-Military International Studies, Strategic Studies and International Security, Geopolitics and Global Security.

ISSN 2532-6570

The recent evolution of this threat in the underwater environment is further aggravated by other factors, such as a lack of accurate definitions that refer to critical infrastructures; the difficulty of exploring the underwater dimension due to its very physical nature; the multitude of potential threats affecting the underwater infrastructures; and the possibility of generating tremendous damage by means that, in some cases, might be simple and economical to build and operate (consider, for example, how cost-effective it is to place a sea-mine to damage a ship).

Economic and technological developments are also bringing about a change in maritime security. Security policies addressing maritime infrastructures traditionally focused on maritime transport (naval bases and sea ports) and the transport of energy resources (gas, oil and hydrocarbons in general). However, in recent years, the number of submarine cables for data transfer has increased enormously, while offshore renewable energy technologies (wind and tidal systems) will incrementally spread in the context of decarbonisation.[4] Furthermore, the future proliferation of unmanned assets and the resulting increase in seabed exploration for energy resources or military applications, coupled with the disruptive advantage brought about by artificial intelligence, could generate both new types of critical underwater infrastructures and new related threats. In fact, NATO and the EU have predicted that, as the number of offshore energy platforms increases, the network of undersea energy infrastructures in the Euro-Atlantic area will grow accordingly.[5] Malevolent actors may leverage these developments to cause damage to underwater infrastructure and assets.

Russian capabilities in the underwater domain

Since the invasion of Ukraine, Russia has become the most significant and direct threat to the security of the NATO allies, a threat that includes the ability to strike their critical infrastructures in the maritime domain, including those in the underwater dimension.[6] Russia's ability to strike critical infrastructure is an important component of Moscow's doctrine and potential escalation.[7] Hybrid tactics have been used for decades by the Kremlin, because they allow to stand up to NATO and to overcome certain Russian weaknesses in conventional military assets.

[4] European Commission, *An EU Strategy to Harness the Potential of Offshore Renewable Energy for a Climate Neutral Future* (COM/2020/741), 19 November 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52020DC0741. See also the European Commission DG Energy website: *Offshore Renewable Energy*, https://energy.ec.europa.eu/node/5681_en.

[5] EU-NATO Task Force on the Resilience of Critical Infrastructure, *Final Assessment Report*, June 2023, https://commission.europa.eu/media/53137_en.

[6] NATO, *2022 Strategic Concept*, June 2022, point 13, https://www.nato.int/strategic-concept.

[7] Michael Kofman, Anya Fink and Jeffrey Edmonds, *Russian Strategy for Escalation Management: Evolution of Key Concepts*, Arlington, Center for Naval Analyses, April 2020, https://www.cna.org/reports/2020/04/russian-strategy-for-escalation-management-key-concepts; Russian Presidency, *Strategy of the National Security of the Russian Federation*, 2 July 2021, https://rusmilsec.files.wordpress.com/2021/08/nss_rf_2021_eng_.pdf; and *Concept of Foreign Policy of Russian Federation*, March 2023.

ISSN 2532-6570

Russia is already able to attack and damage critical underwater infrastructures, either by using military assets designed and appropriately refined to operate in the underwater dimension, or by making use of fishing vessels, merchant ships or even small unregistered boats that are more difficult to monitor and identify. Indeed, Russia has a fleet of submarines that have underwater sabotage capabilities,[8] while GUGI submarines and vessels[9] are mapping underwater infrastructure networks throughout Europe's adjacent seas.[10] The recent spread of unmanned assets, which can even operate covertly, has made the situation even more dangerous.

Furthermore, in the past, the Kremlin has conducted operations through private military companies as well. This might also occur in the undersea environment by employing modified merchant ships, fishing boats armed with equipment capable of snagging gas pipelines and underwater cables, commercial-grade unmanned platforms[11] and unconventional assets. All such means would perfectly fit in a hybrid warfare scenario.

Another option that Russia could implement is to damage underwater infrastructure through mechanical actions. Mechanical damage of submarine cables is a more than a century-old tactic. In fact, at the beginning of World War I, one of the most innovative offensive actions conducted by the Royal Navy was precisely the cutting of German submarine communication cables in the English Channel.[12] Damage to critical underwater infrastructure by mechanical actions is not only possible, it is actually very frequent in the Mediterranean area. It becomes even more critical considering that all underwater infrastructures are visually represented on every nautical chart, and thus accessible to the public.[13]

Regardless of the type of means, way and platforms (manned or unmanned), Russia could potentially already strike critical underwater infrastructures in Europe, which calls for an adequate response by European and NATO allies.

[8] Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Underwater Infrastructures", in *RUSI Commentaries*, 25 May 2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.

[9] Ibid. GUGI is the Russian acronym for *Glavnoye Upravlenie Glubokovodnikh Issledovanii*, which identifies the Russian Directorate, founded in 1965 and operating within the Russian Minister of Defence, responsible for conducting sabotage and surveillance against critical maritime infrastructure.

[10] Morten Soendergaard Larsen, "Russian Ghost Ships Are Turning the Seabed into Future Battlefield", in *Foreign Policy*, 2 May 2023, https://foreignpolicy.com/?p=1111543.

[11] Saverio Lesti and Alessandro Zacchei (eds), *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.

[12] Julian S. Corbett, *Naval Operations 1914-1917*, London, Longmans Green & Co., 1920, p. 128. See also C.R.M.F. Cruttwell, *A History of the Great War, 1914-1918*, 2nd ed., Oxford, Clarendon Press, 1936, p. 187, https://ia902903.us.archive.org/29/items/in.ernet.dli.2015.57902/2015.57902.History-Of-The-Great-War-1914-1918_text.pdf.

[13] The rationale for such publicity is exactly to avoid accidental stranding and to unequivocally establish sea areas where anchoring and related activities are prohibited.

ISSN 2532-6570

How NATO and European countries should respond

Against this backdrop, NATO's new strategic concept includes attacks on critical infrastructures among the cases that can trigger Article 5 for collective defence. Among them, underwater critical infrastructures are probably the most vulnerable to hybrid threats.[14]

In response to these threats, NATO has started actions to monitor pipelines and critical infrastructure of strategic interest. For its part, the European Union has accelerated numerous permanent structured cooperation projects, dispensed economic sanctions which have closed airspace and seaports to Russian vessels,[15] and initiated policies to gain strategic autonomy in energy resources.[16]

Action has also been taken by individual European states. Italy, a highly energy-intensive EU member state that is heavily dependent on resource supply and data traffic, has launched a complex critical infrastructure protection operation called Safe Seabed ("*Fondali Sicuri*"). France has promulgated a new Seabed Warfare Strategy[17] and invested in the defence of the ocean bottom. The United Kingdom has started a new naval programme that has led to the commissioning of two Multi-Role Ocean Surveillance warships dedicated to safeguarding vital seabed telecommunication cables and oil and gas pipelines.[18]

Looking ahead, given the extreme vulnerability of critical infrastructures and the repercussions that damage inflicted to them by malevolent actors could cause to the stability of EU and of the Alliance, it is essential to start a coordinated, synergic and persistent operation of maritime surveillance and presence at sea, in order to be able to gain greater awareness of the maritime – especially underwater – critical infrastructures.

Such action, that may be achieved within the EU, the Alliance or by a coalition of willing, should consist of a joint force, permanently deployed, with the clear strategic objective to deter malicious actions. It should be able to operate in a legal framework supported by multi- or bi-lateral international agreements among riparian states, for the enforcement of restricted areas in proximity of the critical infrastructures to be protected. This would be vital to address the emerging threats in the underwater domain at the time of the Russian war against Ukraine.

18 June 2024

[14] Georgios Giannoulis (ed.), "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.

[15] Anna Caprile and Angelos Delivorias, "EU Sanctions on Russia: Overview, Impact, Challenges", in *EPRS Briefings*, March 2023, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739366.

[16] European Commission website: *European Critical Raw Material Act*, https://commission.europa.eu/node/28722_en.

[17] French Ministry of Armed Forces, *Seabed Warfare Strategy*, February 2022, https://archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf.

[18] "First of Two MROS Ships Arrives in the UK", in *Naval News*, 19 January 2023, https://www.navalnews.com/?p=41591.

ISSN 2532-6570

Istituto Affari Internazionali (IAI)
The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17
I-00186 Rome, Italy
Tel. +39 066976831
iai@iai.it
www.iai.it

Latest IAI COMMENTARIES

Editor: Leo Goretti (l.goretti@iai.it)