

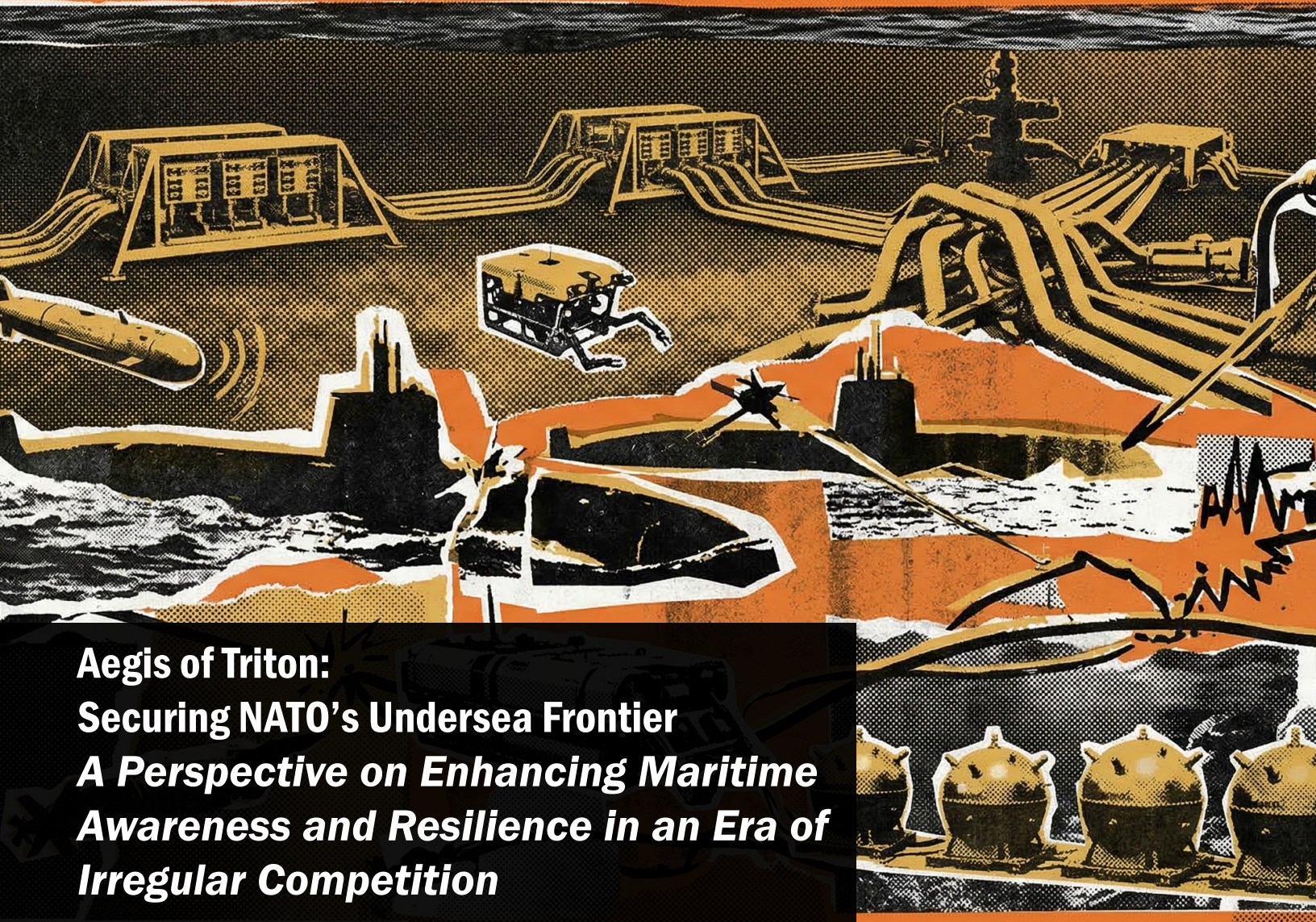
18 March 2026

IW PERSPECTIVE



**IRREGULAR
WARFARE CENTER**

Established October 2022 - Arlington, VA



Aegis of Triton: Securing NATO's Undersea Frontier A Perspective on Enhancing Maritime Awareness and Resilience in an Era of Irregular Competition

Biographies: Tural Akhundov is Master of Political Science from European Humanities University (Vilnius, Lithuania) and Irregular Warfare Center's course graduate. As part of previous work experience in the field of Artificial Intelligence he analyzed the implementation of AI in different spheres. Dr. Maurizio Geri is a former NATO analyst, an Italian Navy Lieutenant POLAD reservist, and a GMU postdoctoral researcher/EU Marie Curie Fellow who specializes in EU-NATO tech cooperation and Russian-Chinese hybrid warfare in the energy-resources-technology security nexus.

ABSTRACT

The undersea environment has become a **critical arena for irregular competition**, as state and non-state actors increasingly engage in covert activities that exploit **gaps in maritime domain awareness**. From intelligence collection and seabed infrastructure interference to clandestine unmanned systems

The views expressed in these articles are those solely of the authors and do not reflect the policy or views of the Irregular Warfare Center, Department of War, or the U.S. Government.



deployment, adversaries often operate **below the threshold of armed conflict, complicating detection, attribution, and response.** These actions challenge NATO's existing mechanisms of maritime domain awareness, as detection, attribution, and response are often constrained by environmental complexity, limited sensing coverage, and communication barriers.

This article argues that current maritime monitoring architectures are insufficient to address the growing strategic significance of the undersea domain in irregular warfare (IW). In particular, gaps in sensing integration, environmental prediction, and secure data transmission reduce the ability of allied forces to identify and respond to anomalous activity in coastal and near-seabed environments.

To address this problem, the article proposes an integrated analytical framework combining environmental modeling, multi-source data fusion, autonomous sensing systems, and secure communication networks. By applying artificial intelligence (AI)-enabled analytics and resilient sensing architectures, such a framework could improve situational awareness, support earlier detection of anomalous behavior, and enhance deterrence-by-denial in contested maritime spaces.

The article concludes that strengthening integrated undersea monitoring capabilities is essential not only for maritime security but also for broader irregular warfare objectives, as increased transparency and predictive capacity can reduce adversary freedom of action in the subsea domain.

Introduction

The Undersea Domain in Modern Irregular Competition

The coastal and subsea environment has emerged as a strategic space for hybrid operations, where adversaries exploit limited visibility, environmental complexity, and legal ambiguity to pursue political and military objectives. Activities such as pipeline sabotage, fiber-optic cable tapping, covert seabed mapping, and

deployment of uncrewed underwater vehicles increasingly characterize state-led gray-zone campaigns. These operations often aim to erode confidence in security guarantees, strain alliance cohesion, or impose economic and political costs without triggering North Atlantic Treaty Organization's (NATO) Article 5 thresholds.

Therefore, maritime domain awareness becomes paramount in the new permanent state of low intensity war. This includes maritime situational awareness, gathering of static and dynamic data for a picture of the situation, maritime threat awareness with the identification of the potential threats that could be active within the area of interest, and maritime response awareness for the mapping and real-time tracking of available response resources. These operations in the maritime domain happen increasingly at the intersection of energy security and technological security. The current transitions in energy and technology in fact make NATO allies more vulnerable and the rivals bolder in their [hybrid-irregular](#) actions, especially in the maritime domain. Therefore, it is important for the NATO alliance to enhance its maritime awareness and resilience, and in order to do that to invest quickly and efficiently in the so called emerging disruptive technologies ([EDTs](#)). These EDTs will help the alliance to develop undersea monitor, prediction, and prevention tools, to deter and defend from possible new attacks in the underwater domain. Today, state actors are increasingly using their shadow fleet not only to evade oil sanctions but also for [covert operations](#) against critical maritime infrastructures. Actually, one of the European Union (EU) naval operations, The European Union Naval Force Mediterranean Operation Irini, since March 2026 includes in its [mandate](#) the maritime situational awareness towards critical maritime infrastructures. This highlights a renewed [cooperation](#) between the EU and NATO could also become important for the future hybridization of conflict in the maritime domain awareness.





Environmental Variability

Coastal and shallow waters present dynamic and [highly variable conditions](#) shaped by currents, tides, salinity changes, temperature gradients, and water-quality fluctuations. For both military operations and adversary monitoring, these factors directly affect detection ranges, acoustic propagation, and the performance of autonomous platforms. [Predictive modeling](#) informed by historical data and real-time sensor input can enable operators to anticipate environmental changes, increasing the effectiveness of maritime patrols, submarine operations, and unmanned underwater vehicle deployment - key components in countering hybrid actions.

Data Collection and Transmission

The undersea domain imposes unique constraints on sensing and communications: Signal attenuation limits the effective transmission range, while restricted bandwidth reduces the amount of data that can be transmitted. In addition, latency may hinder real-time operations and data integrity remains vulnerable to interception or manipulation by hostile actors.

[Effective IW-oriented surveillance](#) therefore requires resilient, secure, and distributed sensing systems capable of fusing data from fixed seabed sensors, autonomous underwater vehicles and remotely operated vehicles, as well as surface buoys, platforms, and satellite-based observations. Secure communication channels whether acoustic, optical, or buoy-relayed, can ensure that valuable intelligence reaches command centers without compromise.



Toward an Integrated Undersea Monitoring Framework

Given the limitations of current monitoring approaches, this article argues for the development of an integrated framework for NATO's undersea situational awareness. Rather than relying on isolated sensing systems, such a framework would combine several complementary technological components to reduce existing gaps in maritime awareness.

- 1. Advanced Modeling and Prediction:** Next-generation hydrodynamic models can assimilate live data streams to [forecast environmental conditions](#) with high temporal and spatial resolution. Machine-learning algorithms would refine predictive accuracy, enabling operators to anticipate adversary movement patterns, optimize Unmanned Underwater Vehicle (UUV) routes, and identify environmental anomalies.
- 2. Multi-Source Data Fusion:** Data integration lies at the core of maritime IW resilience. By unifying information from buoys, autonomous underwater vehicles, satellites, and fixed sensors into a consolidated operational picture, analysts can identify deviations from expected patterns - such as unexplained acoustic signatures, irregular seabed disturbances, or unregistered platform activity. [This fusion approach](#) supports attribution, enhances decision-making, and provides a foundation for rapid response to emerging threats.
- 3. Encrypted and Resilient Data Transmission:** [Secure communication](#) is essential in an environment where adversaries actively target information pathways. The solution could incorporate acoustic modems for subsea communication, buoy-based relay systems to enable extended-range data transfer, and robust encryption protocols to safeguard data integrity. These methods may limit opportunities for eavesdropping or data manipulation while maintaining connectivity in contested electromagnetic environments.



- 4. Submarine Communication Buoy:** Deployable [communication buoys](#) could act as temporary bridges between submerged assets and command nodes. These systems would enable secure burst transmission without compromising submarine stealth - a critical advantage in gray-zone deterrence and covert monitoring missions.

In essence, this strategy for overcoming the difficulties of the coastal and near-seabed environment serves as an example of the synergy between creative thinking and superior technological achievement. By integrating data fusion, encrypted transmission, advanced modeling, and submarine communication, we can get closer to overcoming current constraints and elevate undersea operations expertise.

From Concept to Capability Implementing Pathways

While the need for improved undersea situational awareness is increasingly evident, the transition from conceptual framework to operational capability requires a gradual and carefully managed process. Developing an integrated monitoring architecture for the subsea environment involves not only technological innovation but also institutional coordination, testing, and adaptation to operational realities. For this reason, the implementation of such a system is best understood as a phased process in which analytical capabilities, operational validation, and institutional integration evolve together.

In the initial stage, efforts would likely focus on strengthening the analytical foundations of the system. During this early phase, the primary objective would be to improve the integration of real-time data from multiple sources and refine the environmental models that underpin predictive analysis. Advances in machine learning and data processing could enable analysts to extract deeper insights from large and heterogeneous datasets, improving the system's ability to identify anomalies and forecast environmental changes. At the same time, the development of user-oriented visualization tools would be essential for translating

complex data streams into operationally meaningful information. Providing decision-makers with clear and timely visual representations of undersea conditions would help ensure that analytical improvements translate into practical situational awareness.

A second stage would involve transforming these analytical capabilities into a functioning operational prototype. At this point, the system would evolve from a primarily analytical tool into an integrated software environment capable of supporting real-world maritime monitoring. Testing such a prototype in controlled coastal or near-seabed environments would allow researchers and operators to evaluate its performance under realistic conditions, including fluctuating environmental factors and varying sensor inputs. These pilot deployments would provide valuable feedback on the reliability, responsiveness, and usability of the system. Equally important during this phase would be the gradual integration of the framework into existing maritime information structures. Ensuring compatibility with established monitoring networks and command systems would allow undersea predictive capabilities to complement, rather than duplicate, current maritime awareness efforts. In practical terms, this means connecting new analytical tools with the broader architecture of allied maritime surveillance systems so that undersea insights can contribute directly to operational planning and response coordination.

Over the longer term, the value of such a system would depend on its ability to function across a wide range of maritime environments. Expanding deployments beyond initial test areas would allow the framework to be validated under diverse oceanographic conditions and operational scenarios. As confidence in the system grows, its analytical outputs could increasingly inform maritime planning processes, particularly within naval operations concerned with hybrid threats and irregular maritime activity. Ultimately, the integration of predictive undersea monitoring into strategic decision-making could strengthen the ability of maritime forces to anticipate and counter covert activities targeting critical seabed infrastructure.



Challenges and Considerations

The development of such capabilities also presents several challenges that must be addressed throughout the implementation process. One of the most significant concerns involves the integration of diverse data sources. Combining information from satellites, seabed sensors, autonomous platforms, and environmental monitoring systems introduces technical complexity and raises questions about data consistency and reliability. Addressing this issue requires robust validation procedures and careful preprocessing of incoming data to ensure that predictive models operate on accurate and coherent information.

Another challenge relates to the performance of machine-learning algorithms in dynamic maritime environments. Oceanographic conditions are inherently variable, and predictive models must be continuously refined to maintain their accuracy over time. Regular evaluation and updating of analytical models therefore become essential components of system maintenance, ensuring that predictions remain reliable as environmental patterns evolve.

Finally, the successful adoption of such a framework depends on its compatibility with existing operational structures. Integrating new analytical tools into established naval systems can be difficult if technological development proceeds without close coordination with operational stakeholders. Sustained collaboration between researchers, naval authorities, and maritime security institutions is therefore critical to ensure that emerging capabilities align with real operational needs and can be incorporated smoothly into existing command and decision-making processes.

Taken together, these considerations highlight that improving undersea awareness is not simply a matter of deploying new technologies. Rather, it requires a sustained process of experimentation, validation, and institutional adaptation through which analytical innovation can gradually be transformed into operational advantage.

CONCLUSION

This perspective paper represents a transformative step toward securing NATO's undersea frontier by merging advanced modeling, multi-source data fusion, encrypted communications, and sustainable power-optimization strategies into a single, integrated system. As hybrid threats grow more sophisticated, the ability to interpret, predict, and respond to dynamic undersea conditions in real time becomes not only advantageous but essential. The proposed approach delivers this capability through innovative AI-driven analytics and resilient communication architectures that enhance situational awareness, operational precision, and environmental stewardship.

This article, together with the development roadmap and proposed mitigation strategies, is positioned to potential transition from concept to operational capability. By enhancing transparency in the undersea domain, the paper aims to strengthen deterrence-by-denial and reduce the operational space for malign actors employing hybrid, irregular or covert methods. By leveraging cutting-edge predictive tools and robust data transmission frameworks, the perspective enables faster decision-making, extended operational deployments, and insights that traditional methods fail to achieve. Moreover, its emphasis on energy efficiency and ecological responsibility ensures that technological advancement does not come at the expense of the marine environment.

To secure NATO's undersea frontier in the new era of irregular competition its fundamental to increase the alliance's capabilities and strategies in the maritime domain. The ongoing transitions in both energy security and technological security are increasingly impacting the maritime domain and have heightened the vulnerability of NATO allies while emboldening adversaries to expand their hybrid and irregular activities. In this context, strengthening maritime awareness and resilience has become a strategic imperative for the alliance and investing in new technologies becomes the leverage necessary for the deterrence and defense of our common space.