ON UNDERWATER DATA CENTERS: SURVEILLANCE, MONITORING, AND ENVIRONMENTAL MANAGEMENT IN THE BALTIC SEA

Mark Abner[1], **Sanja Bauk**[2]
[1,2]*Estonian Maritime Academy, Tallin University of Technology (TalTech), Tallinn, Estonia, maabne@taltech.ee*
[2]*sabauk@taltech.ee; bsanjaster@gmail.com, 0000-0003-2882-1321*

Original scientific paper

https://doi.org/10.7251/JIT2402142A UDC: 005.21(261.24):004.946(430:470)

Abstract: This article analyzes underwater surveillance and monitoring technologies aimed at enhancing security and environmental management, using a hypothetical underwater data center in the Baltic Sea as a case study. It explores cutting-edge solutions such as remotely operated vehicles (ROVs), autonomous underwater vehicles (AUVs), and smart buoys, focusing on their integration for monitoring underwater infrastructure and safeguarding against infrastructural threats. With rising concerns over maritime security due to recent events like the Nord Stream outage, this research highlights the need for advanced technological systems to address such a kind of vulnerabilities. The analysis also considers multi-layered potential of these systems for security, safety, and environmental resilience. Consequently, this study provides insights into the feasibility, challenges, and future directions for deploying underwater data centers as a sustainable alternative to traditional land-based facilities of this type, contributing to the broader discourse on securing critical underwater infrastructure and promoting eco-friendly data storage solutions.

Keywords: underwater data center, Baltic Sea, surveillance, monitoring, maritime infrastructure, security

INTRODUCTION

The concept of underwater data centers has gained significant attention in recent years as a potential solution to the growing challenges associated with traditional land-based facilities. The development of underwater data centers is primarily driven by the need to address high energy consumption, environmental impact, and security concerns inherent to conventional data center operations.

This study uses a qualitative research approach to assess the feasibility and risks of deploying underwater data centers, with a focus on the Baltic Sea. A PESTLE - Political, Economic, Social, Technological, Legal, and Environmental analysis framework was employed to evaluate external factors influencing underwater data center deployment. Additionally, a risk matrix assessment was conducted to prioritize potential threats based on their likelihood and impact.

Data was collected through literature reviews, expert interviews, and analysis of industry reports, providing a comprehensive understanding of the political, environmental, and technological challenges specific to underwater data centers. Using the PESTLE framework helped to identify the critical issues.

The rest of the paper is organized in a way that it:

- Gives an overview of history and evolution of underwater data centers;
- Highlights current developments in this domain;
- Underscores the threats to which the Baltic Sea region is currently exposed to;
- Elaborates the role of surveillance and monitoring technologies including Remotely Operated Vehicles (ROVs), Autonomous Underwater Vehicles (AUVs), or, Unmanned Aerial Vehicles (UAVs), and smart buoys, including their integration;
- Analysis the conditions for the development of an underwater data center in the Baltic Sea, concerning environmental, geopolitical, and security risks, along with the legal and regulatory challenges.
- These subtopics are framed at the end with the conclusion part.

Underwater Data Centers

The idea of placing data centers underwater is not entirely new, but it has only recently been pursued on a larger scale. The early 21st century saw increasing awareness of the environmental and economic drawbacks of conventional data centers, which consume vast amounts of electricity for cooling, e.g. As the demand for digital services continued to grow, the industry began to explore alternative approaches to cooling and energy efficiency. One innovative solution emerged in the form of underwater data centers, which leverage the natural cooling properties of the ocean to maintain optimal operating temperatures for servers. For example, over the past few years, data center electricity consumption has accounted for a relatively stable 1% of global electricity usage, excluding cryptocurrency mining [1].

Microsoft's Project Natick, which began in 2013, marked a turning point in the development of underwater data centers [2]. The project aimed to investigate whether a sealed container filled with servers could operate efficiently underwater. The first phase of Project Natick, launched in 2015 off the coast of California, involved a small, prototype data center placed 30 feet underwater for several months. This initial test demonstrated the feasibility of the concept and showed promising results in terms of energy efficiency and reliability.

In 2018, Project Natick entered its second phase with the deployment of a larger underwater data center off the coast of Scotland's Orkney Islands. This new unit, which was the size of a standard shipping container, housed 864 servers and operated entirely on renewable energy sourced from nearby wind and solar farms. The data center was submerged approximately 117 feet below the ocean's surface, where it remained for two years. During this period, the underwater data center exhibited a failure rate that was significantly lower than traditional land-based data centers. The cooler, stable environment and the absence of human interference contributed to the improved performance.

The successful results of Project Natick's second phase solidified the viability of underwater data centers as a sustainable and resilient alternative to conventional approaches (Fig. 1).

Fig. 1. *Microsoft Project Natick 2. Source: [2]*

Existing Underwater Data Centers

Following the success of Microsoft's Project Natick, other companies and organizations have started to explore the potential of underwater data centers. For instance, Subsea Cloud, founded by Maxie Reynolds, offers a commercial underwater data center service that uses liquid immersion cooling technology. Unlike Project Natick, which used a sealed nitrogen-filled environment, Subsea Cloud employs dielectric liquids to cool servers directly, providing even greater efficiency in heat dissipation. Subsea Cloud has active projects the Gulf of Mexico and is looking to expand to the North Sea and the Pacific Ocean [3].

Another major player in the field is the Chinese company Highlander, which, with the backing of the Chinese government, launched the world's first commercial underwater data center near Hainan Island in 2021. The facility can support large-scale computing, and storage needs while utilizing the surrounding seawater for cooling. The 1 400-tonne system is submerged 35 meters on the seafloor and the water is used as natural cooling. Further plans indicate that 100 modules are planned to deploy at the site. It means that it would save 68 000 square meters of land, along with 122 million kilowatt-hours of electricity and 105 000 tons of freshwater per year [4].

These developments highlight the increasing interest in underwater data centers, not just as experimental projects, but as commercially viable and scalable solutions. Albeit, the deployment of underwater data centers introduces challenges, particularly in regions with complex environmental and geopolitical dynamics, such as the Baltic Sea.

Baltic Sea Challenges

The Baltic Sea presents a unique set of challenges for the deployment of underwater data centers due to its environmental characteristics, strategic significance, and actual geopolitical tensions.

The Baltic Sea is a semi-enclosed body of water bordered by several countries, including Estonia, Latvia, Lithuania, Finland, Sweden, Denmark, Germany, Poland, and Russia (Fig. 2). It has distinct environmental features, such as low salinity, limited water exchange with the Atlantic Ocean, and relatively shallow depths. These factors can influence development, operation and maintenance of underwater infrastructure.

One of the cases was Balticconnector gas pipeline and communication cables failure (Fig. 3). Stockholm investigators confirmed that damage to an undersea cable was caused by "means of external force or tampering" [5].

The authorities believe the damage to the pipeline was likely caused by the ship's anchor, but it is not yet known if it was deliberate or unintentional [6]. Therefore, this remains at the level of a suspicion.

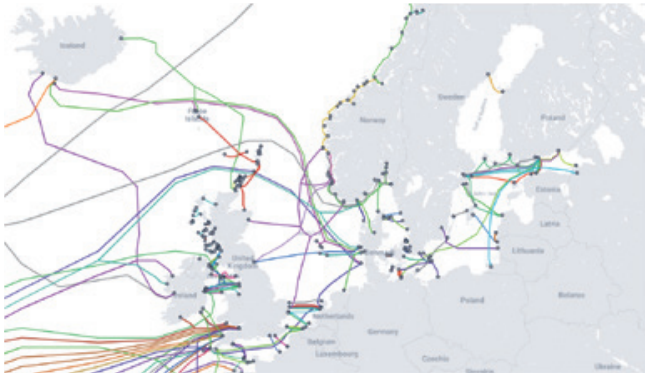

Fig. 2. *Underwater telecomunication cables in Europe. Source: [7]*

Fig. 3. *The damaged offshore Balticconnector gas pipeline. Source: [8]*

Furthermore, due to some recent Twitter (https://x.com/auonsson) reports numerous security incidents are suspected to be sabotage. The Chinese ship, Yi Peng 3, crossed C-Lion 1 and BSC cables at times these were broken (Fig. 4). Then, this ship has been detained by Danish navy on November 19, 2029 (Fig. 5).

However, this is still in a grey area and at the level of a security incident suspected to be sabotage. There have been no official reports from the authorities.

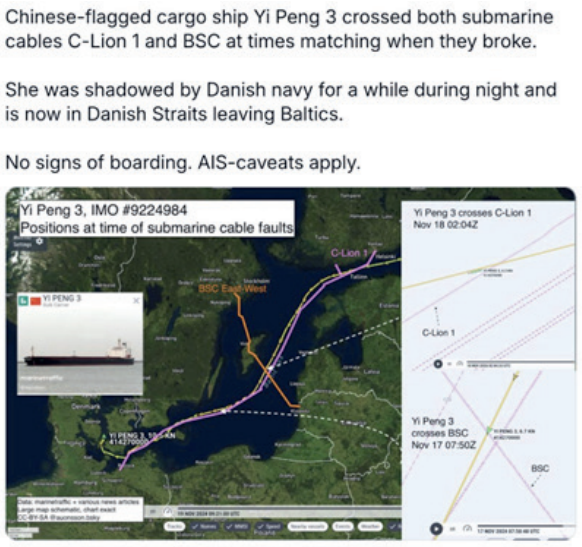

Fig. 4. *Auonsson's post on November 19, 2024. Source: https://x.com/auonsson*

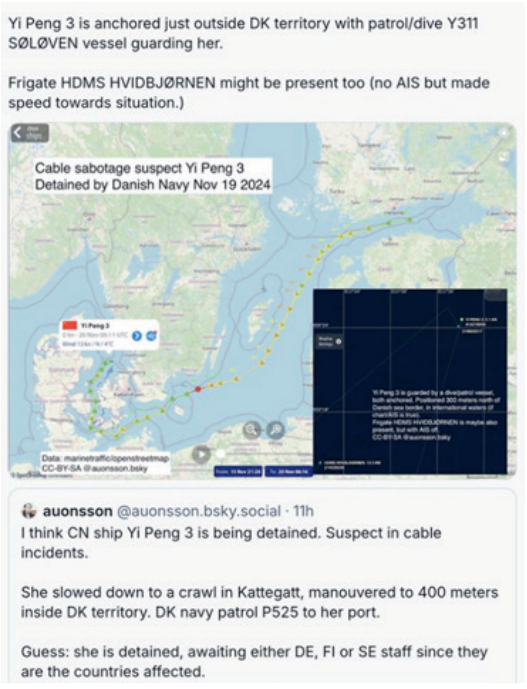

Fig. 5. *Auonsson's post on November 20, 2024. Source: https://x.com/auonsson*

Environmental Factors

The unique environmental conditions of the Baltic Sea, including its low salinity and temperature variations, can affect the performance of underwater data centers. Low salinity may impact the cooling efficiency, while temperature fluctuations could influence the stability of the underwater environment. Additionally, the seabed in some areas is characterized by a mixture of soft sediments, which could pose challenges for anchoring or installing underwater infrastructure. Biofouling, or the accumulation of organisms on submerged structures, is another concern, as it could affect the efficiency of cooling and increase maintenance requirements.

The Baltic Sea is also home to significant marine ecosystems and protected areas, which necessitates careful planning to minimize the environmental impact of underwater installations. The deployment of underwater data centers must consider regulations related to marine conservation, and impact assessments may be required to evaluate potential effects on local wildlife and habitats [9].

Geopolitical and Security Concerns

The strategic significance of the Baltic Sea has been highlighted in recent years due to geopolitical tensions and incidents such as the Nord Stream pipeline outage. As a result, underwater data centers in this area would be exposed to potential security threats, including sabotage, espionage, and cyber-attacks. The security of underwater data centers is a critical consideration, as these facilities could be targeted to disrupt communication networks or compromise sensitive data. Physical security measures, such as surveillance systems and protective enclosures, are essential to safeguard the infrastructure from sabotage. Additionally, robust cybersecurity measures and protocols are needed to prevent unauthorized access to the data center's systems.

Legal and Regulatory Challenges

The legal framework governing underwater infrastructure in the Baltic Sea is complex, with overlapping jurisdictions and international agreements. Countries bordering the Baltic Sea have established Exclusive Economic Zones (EEZs) that grant them certain rights over marine resources and infrastructure.

Involvement of the international waters and shared boundaries complicate the regulation of underwater installations. Regulatory compliance is necessary for the deployment of underwater data centers, and stakeholders must navigate a range of legal requirements related to maritime law, environmental protection, and data security. Coordinating with multiple governments and regulatory bodies can be challenging, especially in a region where political relations may fluctuate.

Surveillance and Monitoring

The use of advanced surveillance and monitoring technologies in undersea area becomes crucial. Technologies such as Remotely Operated Vehicles (ROVs), autonomous underwater vehicles (AUVs), and smart buoys can help detect physical threats, monitor environmental conditions, and ensure compliance with legal and regulatory standards.

An underwater robot connected to a mother ship by a network of cables is called a ROV. An AUV, on the other hand, completes its survey mission without the assistance of an operator. At the end of a mission, the AUV returns to a pre-programmed location so that the data can be downloaded and processed. For monitoring the sea environment (temperature, salinity, or currents), smart buoys serve as stationary or partially mobile nodes. They relay data in real time and assist ROVs and UAVs with navigation. These technologies work together through complementary roles, tasks sharing, and synchronized communication.

The ROVs can examine underwater effects, buoys gather water quality data, and UAVs "keep an eye" on surface algal blooms, e.g. The ROVs find and retrieve underwater targets, while smart buoys offer real-time environmental data and detect surface debris. Smart buoys gather long-term data, while the UAVs map coral reefs and inspect surface infrastructure. The ROVs carry out usually in-depth underwater surveys [10; 11], etc.

Remotely Operated Vehicles (ROVs)

The ROVs are underwater robots that can be controlled from the surface to inspect and maintain underwater infrastructure. Equipped with cameras, sonar, and various sensors, ROVs provide high-resolution imagery and real-time data on the condition of underwater facilities. They are particularly useful for

conducting detailed inspections of underwater data centers, identifying physical threats, and performing maintenance tasks. The ROVs require human operators and they are limited by tether lengths, which can restrict their operational range in deeper waters. Estonian company Flydog Marine has profiler buoy "Mona" and submerged profiler "Salla" (Fig. 6). Technical specification of "Mona" is given in Table 1.

Fig. 6. *Submerged profiler „Salla". Source: [12]*

Autonomous Underwater Vehicles (AUVs)

AUVs operate independently of surface control, using pre-programmed missions and onboard sensors to navigate underwater. For example, ECA Groups A18-M has applications for the defense and security sector encompass: Rapid Environment Assessment (REA); Intelligence, Surveillance and Reconnaissance (ISR); organic underwater mine warfare: mine countermeasures mission module for large multipurpose vessel and mission module for oceanic mine warfare, and conventional underwater mine warfare: detection and classification [12]. They can conduct extensive surveys over large areas, making them ideal for monitoring the surrounding environment and detecting potential threats such as unauthorized vessels. The AUVs are advantageous for long-duration missions and can cover greater distances than ROVs. However, their autonomy poses challenges in real-time communication and data transfer, particularly in deep-sea or high-turbidity conditions. The AUVs are versatile tools for marine surveillance, capable of operating independently across diverse missions, from scientific research to defense applications. The COMPASS2020 project, e.g., showcases AUVs like the A27 and A9-E, highlighting their robust design and advanced capabilities. For instance, the A27 operates at depths up to 300 meters and can carry high-performance payloads, including Synthetic Aperture Sonar (SAS) and multi-beam echo sounders, with a speed range of 3-6 knots. Similarly, the A9-E is optimized for environmental monitoring, offering real-time data on water conditions such as turbidity and pH levels, and features low acoustic signatures to avoid mine detection. These AUVs navigate using Inertial Navigation Systems (INS), Doppler Velocity Logs (DVL), and periodic Global Positioning System (GPS) resurfacing. Equipped with communication options like acoustic, WiFi, and Ethernet channels, AUVs represent a crucial asset for sustained and stealthy underwater operations in complex environments [13].

Table 1. *Technical specifications of a profiler buoy „Mona". Source: [12]*

• Profiling depth – *200m* • Length – *4 m* • Height above water – *2 m* • Diameter – *1,2 m* • Weight – *450 kg* • Comms - *GPRS* • Construction – *float from polyurethane foam covered with hard polyurethane coating, with autonomous lantern and passive radar deflector*	• Hardware Controller & Data-Logger – *integrated* • Software – *web-based user interface for controlling the buoy in real-time* • Customization – *can be altered for specific needs* • Cost – *start from 74 995 €*

The Unmanned Aerial Vehicles (UAVs) are a sort of AUVs. They are invaluable assets in maritime missions, offering real-time surveillance and enhanced situational awareness. The Airbus Zephyr S HAPS, for instance, operates in the stratosphere at altitudes up to 70,000 feet with an impressive endurance of nearly 25 days, combining satellite-like persistence with UAV flexibility. Meanwhile, the Tekever AR5 Life Ray Evolution, a medium-endurance UAV, supports maritime patrols with a 50 kg payload, 16-hour endurance, and a cruise speed of 100 km/h, effectively covering large surveillance areas with EO/IR sensors. These UAVs improve maritime security by tracking illegal activities, monitoring environmental changes, and ensuring rapid response in emergencies. Notwithstanding, challenges such as high operational

costs, vulnerability to adverse weather, and integration complexity must be addressed to optimize UAV deployment in maritime operations. Future advancements in UAVs autonomy, durability, and communication capabilities will be essential for even more reliable and resilient maritime surveillance [14; 15].

Smart Buoys

Smart buoys serve as stationary surveillance platforms that can be deployed around underwater data centers to monitor environmental conditions and detect anomalies. Equipped with various sensors, including hydrophones, cameras, and water quality detectors, smart buoys can continuously gather data on water temperature, salinity, and acoustic signals. This capability enables early detection of intrusions or environmental hazards (Fig. 7). Smart buoys are effective for monitoring fixed areas, their coverage is limited, and they may require periodic maintenance and calibration [16; 17].

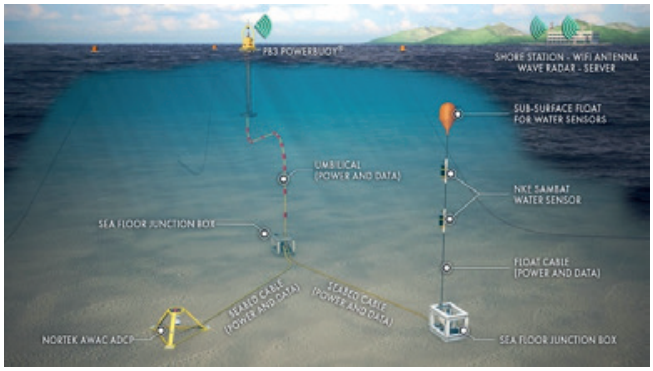

Fig. 7. *Illustration of PB3 Power Buoy environment. Source: [16]*

Underwater Infrastructure Support

The need for specialized monitoring and support services has become essential. Maritime research and surveillance companies offer vital expertise in surveying, inspection, and environmental monitoring for underwater infrastructure. For instance, Reach Subsea [18] company provides comprehensive geophysical and environmental monitoring, leveraging advanced subsea technology to ensure safety, stability, and operational compliance. Its Reach Remote Project emphasizes sustainable, low-emission operations, enhancing access to remote areas. Through real-time and autonomous monitoring solutions, companies like Reach Subsea, help maintain underwater infrastructure integrity in challenging marine environments. Their wide portfolio includes environmental and geophysical monitoring, remote and autonomous fleet, survey and positioning.

Since NATO's inception in 1949, collaborations among the Baltic Sea countries have bolstered environmental and military standards to maintain regional stability. The 2022 Nord Stream outage incident heightened the need for robust security, leading to creation of the Maritime Centre for the Security of Critical Undersea Infrastructure in 2023. Key initiatives include increased patrols, minehunters, drones, and advanced surveillance by NATO and individual Baltic countries. Estonia's "MEREHUNT" smart buoy project also supports coastal monitoring and maritime environmental data, while NATO's Digital Ocean program integrates digital solutions to enhance situational awareness from seabed to space [19; 20]. A map application with an overview of Estonian coastal and offshore stations. Indicative locations and test areas of the new smart buoys are marked with blue circles (Fig. 8).

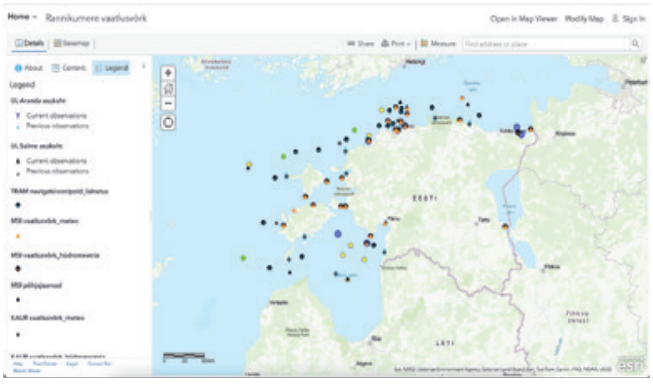

Fig. 8. *Indicative locations and test areas of the new smart buoys. Source: [18]*

The Baltic Sea is subject to various national jurisdictions and international agreements, making legal compliance a significant concern. Surveillance and monitoring systems should be designed to meet the environmental regulations of all bordering countries, including requirements for marine conservation and underwater infrastructure safety. Therefore, compliance with international maritime law is necessary, particularly regarding data center deployment in the EEZs (Fig. 9).

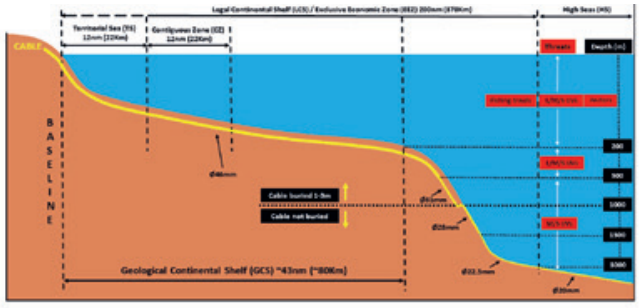

Fig. 9. *Different zones of juridical zones for coastal competence. Source: [21]*

Security Threats

Given the operational and environmental constraints of underwater data centers, international sabotage targeting these facilities can have serious consequences. Due to their heavy reliance on underwater infrastructure, these data centers—which are built for effective cooling and minimal environmental impact—are susceptible to sabotage in several ways. Some examples of sabotage are as follows:

- To cut or damage the communication and power cables that connect it to the shore.
- The use of explosives to breach the data center's pressure vessel or protective casing.
- Interference with pipelines or cooling systems that are utilized for operations and maintenance, etc.

The impacts might be disconnection, which makes the data center unusable; permanent harm from water intrusion to delicate servers and equipment; high expenses for service restoration, recovery and repair, etc. For instance, even sounds from military-grade sonar on ships, submarines, or even whales could interfere with underwater data centers being built off the coasts of China, the US, and Europe [22].

CONCLUSION

The concept of underwater data centers represents a promising alternative to traditional land-based facilities, offering benefits in energy efficiency, environmental sustainability, and security. The successful implementation of projects like Microsoft's Project Natick has demonstrated the feasibility of using underwater environments to reduce cooling costs and improve the resilience of data storage infrastructure. However, deploying a such facility in the Baltic Sea, requires careful consideration of environmental, legal, cyber, and geopolitical issues.

The underwater data center enables comprehensive monitoring, real-time data acquisition, and prompt detection of potential threats, thereby enhancing the security and operational stability of the underwater infrastructure. Security measures must account for the potential risks of sabotage, espionage, and legal disputes. A robust surveillance system that integrates multiple technologies, such as ROVs, AUVs and smart buoys, is crucial for ensuring the data center's safety.

While underwater data centers offer significant advantages, their deployment in sensitive regions requires a careful balance between technological innovation, cyber-risks, environmental protection, and geopolitical challenges. The recommended multi-tiered surveillance strategy can mitigate risks, support legal compliance, and contribute to the sustainable development of a such data center in the Baltic Sea.

Acknowledgement

This research was supported by the EU Horizon2020 project 952360-MariCybERA.

REFERENCES

[1] A. de Vries, "The growing energy footprint of artificial intelligence," *Joule CelPress*, July 7, 2023. [Online], Available: https://www.cell.com/joule/pdf/S2542-4351(23)00365-3.pdf [Accessed Nov. 20, 2024].

[2] Microsoft, "Project Natick Phase 2", n.d. [Online], Available: https://natick.research.microsoft.com/[Accessed Nov. 20, 2024]

[3] P. Judge, "Subsea Cloud announces three underwater data center projects," *DCD*, September 01, 2022. [Online], Available: https://www.datacenterdynamics.com/en/news/subsea-cloud-announces-three-underwater-data-center-projects/#:~:text=Subsea%20Cloud%2C%20the%20company%20proposing,near%20Port%20Angeles%2C%20Washington%20State. [Accessed Nov. 20, 2024]

[4] S. Moss, "China deploys 1,400-ton commercial underwater data center," *DCD*, November 27, 2023. [Online]. Available: https://www.datacenterdynamics.com/en/news/china-deploys-1400-ton-commercial-underwater-data-center/ [Accessed Nov. 20, 2024]

[5] M. Zhang, "Underwater Data Centers: Servers Beneath the Surface," *Dgtl Infra*, January 23, 2024.[Online], Available: https://dgtlinfra.com/underwater-data-centers-servers/ [Accessed Nov. 20, 2024]

[6] EER News, "Cable between Estonia, Sweden damaged by "external force or tampering," *ERR.ee*, October 23, 2023. [Online], Available: https://news.err.ee/1609142222/cable-between-estonia-sweden-damaged-by-external-force-or-tampering [Accessed Nov. 20, 2024]

[7] TeleGeography, "Submarine Cable Map," *TeleGeography*, n.d. [Online], Available: https://www.submarinecablemap.com/[Accessed Nov. 20, 2024]

[8] RAJA, "Rajavartiolaitokselle ja Merivoimille hätäapurahoitusta EU: lta Balticconnector-kaasuputken tutkinnassa tukemisen kuluihin," *RAJA*, April 9, 2024. [Online], Available: https://raja.fi/-/eu-hataapurahoitusta-balticconnector-kaasuputken-tutkinnassa-tukemisen-kuluihin [Accessed Nov. 20, 2024]

[9] A. Mark, " Underwater surveillance and monitoring technologies for enhanced security and environmental management: an analysis of a hypothetical underwater data centre in the Baltic Sea," *Master Thesis*. Tallinn University of Technology, 2024.

[10] J. Hsu, "What is the difference between an AUV and a ROV?," *NOAA-National Ocean Service*, n.d. [Onilne]. Available: https://oceanservice.noaa.gov/facts/auv-rov.html#:~:text=An%20AUV%20conducts%20its%20survey,by%20a%20series%20of%20cables [Accessed Nov. 27, 2024]

[11] M. Babić, M. Oreč and N. Mišković, "Developing the concept of multifunctional smart buoys," OCEANS 2021: San Diego – Porto, San Diego, CA, USA, 2021, pp. 1-6, doi: 10.23919/OCEANS44145.2021.9705916.

[12] Flydog Marine, "Advanced solutions for environmental monitoring," *Flydog Marine*, n.d. [Online], Available: https://www.flydogmarine.com/ [Accessed Nov. 20, 2024]

[13] S. Bauk, "Performances of Some Autonomous Assets in Maritime Missions," *TransNav – International Journal on Maritime Navigation and Safety of Sea Transportation*, Vol.14, No.4, December 2020, pp. 875-881. DOI: 10.12716/1001.14.04.12

[14] S. Bauk et al., "Advantages and disadvantages of some unmanned aerial vehicles deployed in maritime surveillance," *Journal of Maritime Research*, 2020, 17(3), pp. 81–87, https://www.jmr.unican.es/index.php/jmr/article/view/635

[15] S. Bauk et al. (2021). Key Features of the Autonomous Underwater Vehicles for Marine Surveillance Missions. In: Bauk, S., Ilčev, S.D. (eds) *The 1st International Conference on Maritime Education and Development*. Springer, Cham. https://doi.org/10.1007/978-3-030-64088-0_7

[16] OPT-Ocean Power Technologies, "PB3 PowerBuoy," *OPT*, n.d. [Online], Available: https://oceanpowertechnologies.com/platform/opt-pb3-powerbuoy/ [Accessed Nov. 20, 2024]

[17] OPT-Ocean Power Technologies, "Demonstration of OPT PB3 PowerBuoy® Capabilities," *OPT*, February 26, 2019. [Online Video], Available: https://www.youtube.com/watch?v=WyiR_vtRR_M [Accessed Nov. 20, 2024]

[18] ReachSeabed, "Reach Subsea," *ReachSeabed*, n.d. [Online], Available: https://reachsubsea.no/[Accessed on Nov. 20, 2024]

[19] J. E. Hillman, "Securing the Subsea Network: A Primer for Policymakers," *CSIS*, March 9, 2021. [Online], Available: https://www.csis.org/analysis/securing-subsea-network-primer-policymakers [Accessed Nov. 20, 2024]

[20] NATO, "NATO Digital Ocean Industry Symposium - 16-17 April 2024," *NATO Web News*, n.d. [Online], Available: https://www.nato.int/cps/en/natohq/news_219535.htm [Accessed Nov. 20, 2024]

[21] D. Eleftherakis, and V-B. Raul. 2020. "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors", *Sensors* 20, no. 3: 737. https://doi.org/10.3390/s20030737

[22] J. Hsu, "Underwater data centers could be destroyed by loud noises," May 14, 2024, *NewScientist*, May 14, 2024. [Online], Avalilable: https://www.newscientist.com/article/2430616-underwater-data-centres-could-be-destroyed-by-loud-noises/[Accessed on Nov. 27, 2024]

Received: November 22, 2024
Accepted: November 23, 2024

About the authors

Mark Abner holds a master's degree in Maritime Digitalisation and a bachelor's degree in Maritime Transport and Port Management. He has been at the forefront of innovative digital solutions, particularly in the design of underwater data centres. Her master's thesis explored the viability and technological framework required to implement these pioneering facilities. Alongside his academic and professional pursuits, he maintains a robust commitment to endurance sports such as Nordic skiing, cycling and running, underlining a personal commitment to resilience and continuous improvement. This blend of technical acumen and physical endurance uniquely positions Mark Abner to tackle and transform the challenges of maritime logistics and port management.

Sanja Bauk is a Research Professor at the Estonian Maritime Academy within the Tallinn University of Technology. In addition to research, she teaches Introduction to Computer Systems for Maritime Specialist at master's level and Digital Transformation of Maritime Industry at PhD level. Previously, she was an Associated Professor at the Durban University of Technology in South Africa, where she was a researcher and lectured Electronic Navigation, Logistics and Research Methodology. She started her career at the Maritime Faculty of the University of Montenegro in Kotor, where she taught Operations Research and Information Technologies in addition to research. She has a rich and diverse international career, along with a high publication record. Her research interests are multi-layered with a focus on maritime digital transformation.

For citation

Mark Abner, Sanja Bauk, On Underwater Data Centers: Surveillance, Monitoring, and Environmental Management in the Baltic Sea, *JITA – Journal of Information Technology and Applications, Banja Luka*, Pan-Europien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 14(2024)2:142-149, (UDC: 005.21(261.24):004.946(430:470)), (DOI: 10.7251/JIT2402142A, Volume 14, Number 2, Banja Luka, December (89-188), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004