

Security of Maritime Infrastructure

Date: Monday, 28 April 2025

Theme: Sustainable Maritime Infrastructure

Welcome and Introduction

The session “Security of Maritime Infrastructure” gathered experts, researchers, and stakeholders to address the growing threats to critical infrastructure in the Baltic Sea Region. The discussion focused on hybrid threats, vulnerabilities of undersea and offshore infrastructure, and the role of research and innovation in strengthening maritime security.

The session opened with reflections on the rising number of incidents targeting critical maritime infrastructure, such as offshore wind farms and undersea cables. Against this backdrop, participants emphasized the urgent need for a comprehensive, coordinated security approach in the Baltic Sea, involving technical, operational, and governance solutions.

It was noted that damage to infrastructure in one country could have cascading impacts across the entire region, underscoring the interdependence of Baltic states. New initiatives like NATO’s “Baltic Sentry” were highlighted as steps towards stronger regional protection frameworks.

Keynote Presentation

Dr. Radosław Tyślewicz (Polish Naval Academy in Gdynia) delivered a keynote on the vulnerabilities of offshore wind farms in the Baltic Sea. He described how these sites, while crucial for Europe’s energy transition, are exposed to both physical and hybrid threats, including unauthorized access and disinformation campaigns. The need for technical monitoring systems and improved resilience measures was emphasized.

Presentations

- Dr. Cezary Mazurek (Poznan Supercomputing and Networking Center, GÉANT Board of Directors) presented the role of research and secure digital networks in protecting critical infrastructure. He emphasized Europe’s positioning as an “AI Continent,” leveraging supercomputers, quantum computing, AI factories, and common data spaces to support secure and innovative solutions. Submarine cables were identified as vital infrastructure for connectivity and international data transfers, requiring innovative protection measures.
- Dr. Marcin Kowalski (Military University of Technology) introduced VIGIMARE, a Horizon Europe funded research project focused on maritime surveillance and situational awareness, integrating technological and military approaches to monitor and secure maritime assets and activities.
- Dr. Monika Wysocka (Polish Naval Academy in Gdynia) reflected on opportunities to strengthen international scientific cooperation to address shared security challenges in the Baltic.

Key Discussion Points and Conclusions

- Incidents targeting critical maritime infrastructure have significantly increased since 2022, with hybrid threats posing complex risks.
- Offshore wind farms face unique security challenges in multi-use sea spaces, where activities like fishing may pose unintended risks.
- There is a shared recognition that protecting infrastructure like submarine cables—which carry 99% of international data traffic—is critical for Europe’s economic and security interests.
- Participants called for better predictive tools, technical monitoring, and collaborative regional protocols to address security gaps.
- Research and innovation were seen as essential drivers for developing both technical solutions and governance models that facilitate cross-border collaboration while safeguarding national interests.
- Emphasis was placed on leveraging Europe’s investments in AI and digital infrastructures to enhance maritime security through secure networks and shared data spaces.
- A key challenge highlighted was balancing the interconnectedness of critical infrastructure with national sovereignty, requiring trust and cooperation across sectors and borders.

Takeaways and Action Points

1. Strengthen Maritime Security in the Baltic Sea Region: Develop a coordinated strategy to address rising hybrid threats, secure offshore wind farms, and improve risk prediction and mitigation (e.g., addressing risks such as fishermen navigating close to offshore wind farms in multi-use areas).
1. Protect and Make Critical Submarine Infrastructure More Resilient: Enhance the resilience of submarine cables against growing threats through innovation and coordinated monitoring efforts.
1. Boost Research and Secure Networks: Leverage EU advances in AI, quantum computing, and common data spaces to build secure, real-time maritime security systems. The EU's AI Continent Action Plan was highlighted as a positive example.
1. Safeguard EU Interests at Sea: Strengthen coastal patrols and information-sharing platforms (e.g., CISE, MARSUR) to protect trade routes, critical infrastructure, and marine resources.