By Mario Eisenhut,
Mario Eisenhut, Founder, Eisenhut Consulting

A TURNING POINT IN MARITIME SECURITY

PART TWO – A SHIFT IN THINKING

In this second part of a three-part series, Mario Eisenhut discusses sabotage and a shift in thinking. Part 3 will be published in our Q4 issue and Eisenhut will look to the future and make recommendations about the path forward for maritime security.

Since January 2025, a series of incidents have served as a loud wake-up call for the world. In the Baltic Sea, an important fiber-optic cable connecting Sweden and Estonia was intentionally cut, disrupting data flow across the region and stirring diplomatic tensions throughout Europe. Intelligence reports indicate that the operation was carried out with military-like precision and coordination, though no one has publicly claimed responsibility. This event emphasizes just how vulnerable critical undersea infrastructure has become and emphasizes the increasingly advanced and dangerous tactics used to attack global communication networks. It's a clear sign that we need to prioritize the security of these systems as threats evolve.

January 2025: Baltic Sea Sabotage and the New Face of Infrastructure Warfare

The year started with a shock when the EstLink 2 subsea power cable – critical for sending electricity between Finland and Estonia – was mysteriously cut in the Baltic Sea. At first, it seemed like an accident, but investigators quickly zeroed in on the Russian-linked oil tanker Eagle S, which was behaving oddly near the cable's path. Satellite images and marine investigations showed that the ship's anchor had been dragged, pointing to deliberate tampering. Finnish security officials confirmed that this was no simple mishap, but a targeted act meant to test how well the region could handle such disruptions. This incident had serious consequences, shaking up regional energy markets and raising alarms within NATO. It revealed how easily civilian maritime infrastructure can be exploited for strategic purposes. More importantly, it exposed the lack of proper legal measures to prevent or respond to these kinds of attacks. The event was a wake-up call, showing how modern conflicts can weaponize critical infrastructure, and it emphasizes the urgent need for better protection and international cooperation to defend maritime assets.

February 2025: Taiwan's Cable Sabotage and the Gray Zone Strategy

Just a few weeks later, tensions in the Indo-Pacific grew even more. Taiwan detained the Hongtai, a Togolese-flagged ship with a Chinese crew, after an undersea cable connecting Taiwan to its strategically important Penghu Islands was cut. This was already the second similar incident in less than a month, sparking suspicions of repeated sabotage disguised as normal commercial activity. When inspectors examined the ship, they found signs that indicated deliberate contact with the seabed cable. Taiwanese officials condemned the act, labeling it part of China's "gray zone" tactics — subtle, non-military actions designed to destabilize without directly provoking military conflict. As Taiwan responded by strengthening its defenses, analysts warned that such cable cuts could become a new, sneaky way to pressure and influence cross-strait relations, with serious implications for regional stability and the safety of undersea infrastructure.

March 2025: Cable Attack Emphasizes Growing European Infrastructure

Concerns in March, a troubling incident unfolded when a key undersea cable linking Germany and Finland was damaged — raising new worries about Europe's critical infrastructure. The damaged cable, found near Swedish waters, caused momentary power outages across parts of Central Europe.

Divers later confirmed signs of sabotage, including scratched metal and moved fiber bundles, like previous attacks. Authorities also observed a suspicious vessel nearby that didn't have any flags and managed to avoid being identified before security responded. In response, Sweden, Germany, and Finland quickly coordinated their security efforts, while the European Commission called an emergency meeting in Brussels. It became clear that these events weren't just random accidents but part of a coordinated effort testing Europe's resilience. The Baltic attack added momentum to calls for a unified European Subsea Security Command and renewed debates within NATO on how prepared they are for unconventional threats, especially in maritime areas.

April 2025: U.S. Halts Empire Wind Project Amid Security Concerns

In April, attitudes toward offshore energy infrastructure shifted in the United States — not because of foreign sabotage, but due to domestic security worries. The Biden administration suddenly paused work on the Empire Wind project, which was supposed to be one of the biggest offshore wind farms in the country. While officials cited regulatory problems, insiders hinted that broader national security issues played a big part in the decision. There were reports of military radar jamming, foreign vessels operating near U.S. offshore zones, and growing tensions between energy goals and national defense. Although no direct sabotage was detected, the halt signaled a new understanding: offshore energy installations are now seen as potential strategic vulnerabilities, not just economic assets. Critics argued that this move was a concession to fossil fuel interests, but defense experts saw it as prudent — an important reassessment of security risks. Regardless of the reasons, the decision sent ripples through the renewable energy sector, hinting that future offshore projects might face increased security checks that go beyond normal environmental rules.

A Global Wake-Up Call

The first four months of 2025 have shown a clear and worrying trend: critical maritime infrastructure, which once seemed secure

and mostly hidden, is now becoming a key battleground for global influence. The methods used are both sneaky and highly advanced, including shadow fleets with their transponders turned off, sabotage at anchor points, underwater drones, and powerful signal jamming.

These tactics show a shift in how nations project maritime power — moving toward covert, tech-enabled strategies that make detection and attribution difficult but pose serious risks to global security and critical infrastructure. From the Baltic Sea to the Pacific, these disruptions aren't just random incidents, they're part of a larger pattern.

These alerts are strategic warnings. The mix of cyber, electronic, and physical breaches into essential marine systems calls for an immediate and united global effort. As our world moves faster into digital technology, cleaner energy, and more decentralized systems, the significance of undersea cables and offshore networks has skyrocketed — and so has their vulnerability. What became clear in 2025 is straightforward: the next crisis might not come with loud explosions or traditional battles, but rather through quiet disruptions like a fiber-optic cable being cut deep under the ocean. Together, these events emphasize a worrying trend: our maritime infrastructure is no longer safe from secret attacks. The way conflicts happen today is changing, and our defenses haven't kept up with the pace needed to protect these critical assets. As we grow more dependent on undersea systems, so must our efforts to defend them from increasingly clever and subtle threats.

Geopolitical Dynamics: Maritime Infrastructure as a Strategic Power Lever

For people working in maritime transport, the oceans have long been the backbone of global trade. Ports, shipping routes, and underwater infrastructure may often go unnoticed, but they're what keep our economy moving behind the scenes. These essential pathways are now facing new risks, especially as countries compete more fiercely and hybrid warfare tactics become common. In today's world, the safety of maritime infrastructure is more important than ever, and its vulnerabilities are a growing concern amid rising tensions and new kinds of threats.

Countries like China and Russia have made huge strides in developing advanced underwater technologies. These aren't just for exploring the depths or conducting research, they're increasingly used for strategic purposes, such as controlling critical areas or interfering with networks. From highly sophisticated submarines capable of stealth operations to underwater drones that can map cables or sabotage key targets, maritime infrastructure has become a major point in geopolitical rivalry. These investments are part of long-term strategies to influence essential chokepoints, fiber-optic internet cables, and energy pipelines — giving these nations more use over global markets and security.

For those working in shipping, logistics, port management, or insurance, this shifting threat environment calls for immediate action and strategic planning. The industry isn't only dealing with weather or piracy anymore; it's facing threats related to state-sponsored technological conflicts. As rival powers compete beneath the waves, maritime businesses find themselves on the front lines of a new kind of conflict, where infrastructure that once seemed minor now sits at the center of strategic vulnerabilities. The underwater infrastructure supporting the internet, global finance, shipping logistics, and energy supplies is one of the most critical — and vulnerable — parts of modern civilization. Even a single disruption to subsea fiber-optic cables, which often connect at key maritime hubs, can cause serious ripple effects: halting real-time tracking, delaying cargo updates, and disrupting port operations. Similarly, underwater energy links — like gas pipelines and offshore power lines — are becoming more exposed, risking regional energy stability.

As these systems grow more essential to daily life worldwide, protecting them must be a top priority for nations and international groups. While authoritarian countries benefit from centralized control and long-term planning, democratic nations often face fragmented rules, complex regulations, and uneven resources, leaving essential underwater infrastructure more exposed. This imbalance creates major risks not just for individual nations but for the stability of global trade and logistics networks. For the maritime industry, underwater infrastructure can no longer be seen as a background concern. It's a frontline asset that, if compromised, could cause major disruptions, raising insurance costs, delaying shipments, and threatening supply chains overall. In today's interconnected world, safeguarding these systems is critical to maintaining both business continuity and national security. TSI

About the Author:

Mario Eisenhut is a maritime professional with experience that includes diverse roles across multiple maritime projects. Eisenhut's career has included positions such as marine coordinator, risk advisor, yacht service manager, business development manager, project manager and captain. He is skilled in risk analysis, with hands-on experience as a test manager for drone operations, focusing on safety management. Currently he is serving as a marine coordinator in the North Sea, overseeing ship activities, managing permits and ensuring operational seamlessness. He can be reached at m.eisenhut@consulting-eisenhut.de.

Reach over 177,000 Transport Security Professionals Instantly with

TSI TRANSPORT SECURITY INTERNATIONAL

READ LATEST ISSUE **TSI-MAG.COM/CURRENT**

The ONLY dedicated global transport security publication

Trusted by transport security professionals for 25+ years

Published quarterly in print and all digital formats

Get your personalized advertising quote *today!*

2025 Media Pack

Sam Stokes
Publishing Director
+44 (0) 20 3892 3056
sstokes@asi-mag.com

Daniel Goodwin
Sales Director
+1 920 214 0070
dgoodwin@aerospace-media.com

www.tsi-mag.com/advertise

INTERNATIONAL SECURITY EXPO

30 SEPT - 1 OCT 2025 | OLYMPIA, LONDON

CONNECTING THE GLOBAL SECURITY COMMUNITY

10,000+
GLOBAL SECURITY DECISION-MAKERS

300+
INTERNATIONAL EXHIBITING BRANDS

HIGH-LEVEL
SUMMIT & CONFERENCE

EXCITING
LIVE DEMONSTRATIONS

SCAN TO REGISTER FOR FREE

CO-LOCATED WITH

INTERNATIONAL CYBER EXPO
30 SEPT – 1 OCT 2025 | OLYMPIA, LONDON

INTERNATIONALSECURITYEXPO.COM