

Ocean Robotics Planet

Supported by



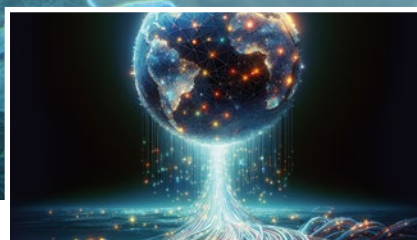
CRITICAL UNDERSEA INFRASTRUCTURE PROTECTION

CUI

SPECIAL REPORT



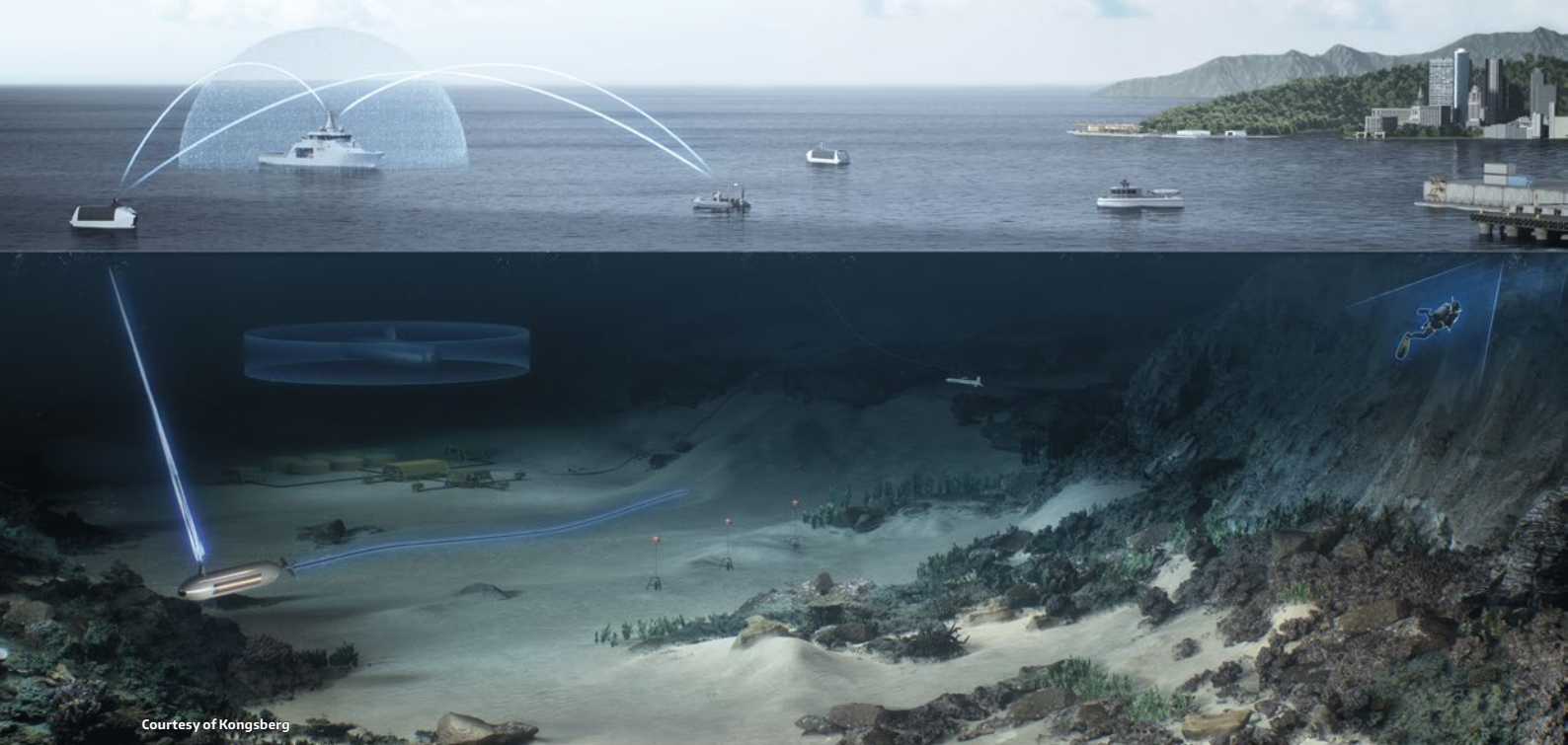
2. KONGSBERG sets CUI milestone with new Oslofjord test bed for safeguarding key assets



6. Dual-Use Dilemma: How Dual-use Tech Is Fueling Military Threats Below the Surface



9. Surveillance network: NATO's Baltic Sentry Builds Connections to Counter CUI Threat



KONGSBERG SETS CUI MILESTONE WITH NEW OSLOFJORD TEST BED FOR SAFEGUARDING KEY ASSETS

As threats to critical undersea infrastructure grow in complexity and scale, Norwegian technology group KONGSBERG has launched a dedicated facility to support the development and testing of integrated protection solutions. This article explores the capabilities and strategic purpose of the new Oslofjord CMI Protection Test Bed – and its role in strengthening Europe’s maritime resilience.

The deliberate sabotage of Nord Stream 1 and 2 in 2022 was a strategic wake-up call for Europe’s energy and security communities. It underscored a vulnerability of critical undersea infrastructure (CUI) that had long been underestimated. Gas pipelines, communication cables, power lines, offshore energy systems – these deepwater assets are not only vital to economic and operational continuity but also increasingly exposed to interference, degradation and direct attack.

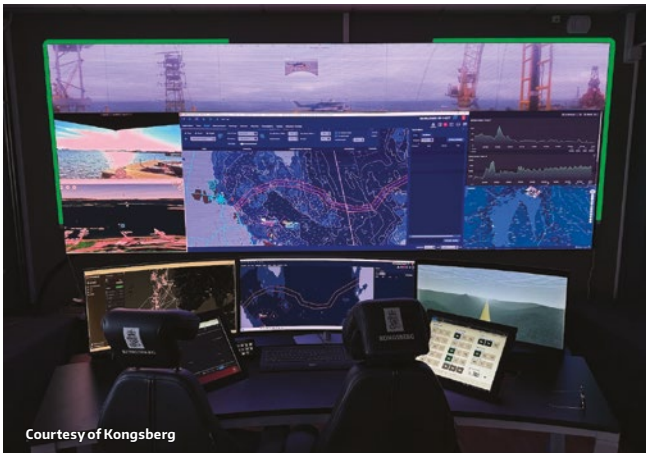
In response to this rising risk, KONGSBERG has established a unique facility in Horten designed to accelerate technological readiness, multi-agency coordination and capability integration. Officially launched on 30 June 2025, the Oslofjord Critical Maritime Infrastructure (CMI) Protection Test Bed serves as a real-world testing ground for the advanced tools, systems and response frameworks needed to safeguard subsea (and surface) infrastructure in a more volatile world.

“With ongoing geopolitical uncertainty and an increasingly dynamic risk picture, the need for safeguarding Critical Maritime Infrastructure has never been greater,” says Geir Håøy, CEO of KONGSBERG. “This centre reflects our commitment to readiness through technology, and to working closely with ecosystem stakeholders to build the robust solutions infrastructure protection demands.”

A CHANGING THREAT ENVIRONMENT

Critical maritime infrastructure – often unmanned, widely spread and difficult to access – now faces a broader set of threats than ever before. These include not only state-sponsored sabotage but also low-cost hybrid operations involving spoofing and jamming, unauthorised seabed activity or the coordinated use of cyber and physical disruption modes. Subsea infrastructure failures are also increasingly linked to equipment age, accidental anchor strikes, cable abrasion and climate-driven seabed changes.

In parallel, maritime traffic has become more complex and difficult to monitor. The rise of the so-called “dark fleet” – sanctions-busting vessels typically operating without AIS transponders – has made it harder to assess risk in the vicinity of sensitive undersea assets. While surveillance and detection technologies have improved, many authorities and operators still struggle to convert wide-area sensor inputs into clear, actionable decisions.



As flagged in the Norwegian government's White Paper on Total Preparedness: Preparing for Crisis and War (published January 2025), there is an urgent need for more robust situational awareness, improved public-private cooperation and enhanced capabilities for real-time monitoring and post-incident response.

This urgency has also been echoed in Brussels. In the wake of the Nord Stream sabotage, European Commission President Ursula von der Leyen stated: "We will step up our protection of critical infrastructure through increased preparedness, resilience and international cooperation."

The political momentum triggered by that event has since led to a series of cross-border initiatives, including the EU-NATO Task Force on the Resilience of Critical Infrastructure and the adoption of the Critical Entities Resilience Directive (CER). These frameworks explicitly identify subsea infrastructure as strategic assets requiring more active protection. They also highlight a persistent capability gap: the lack of integrated test environments where technologies can be evaluated under operationally realistic maritime conditions.

The Oslofjord CMI Test Bed was developed in direct response to this need. It offers a dedicated arena where surveillance, inspection and response systems can be brought together, tested and evolved, supporting both national objectives and Europe's collective preparedness.

OPERATIONALLY REALISTIC TEST ENVIRONMENT

The facility offers a controlled but realistic maritime zone in which stakeholders can test equipment, rehearse incident scenarios, integrate data systems and evaluate new technologies in a live environment.

It is connected to a live network of coastal radars, satellite AIS feeds, seabed sensors and underwater assets – giving users access to a continuous flow of real data. This allows developers and operators to simulate threat events and validate how different systems respond in concert.

Unlike closed labs or short-term demonstrations, the test bed supports extended operations, multi-agency drills, cross-domain system testing and scenario-based evaluations. KONGSBERG has also opened the facility to partner organisations – including energy operators, defence bodies, R&D institutes and regulatory agencies – allowing them to trial their own equipment or validate compatibility with larger protection frameworks.

"The test bed gives us a practical environment to test how sensors, analytics, platforms and human decision-making interact – not in theory, but in context," explains Håøy.

FROM STRATEGY TO STRUCTURE: KONGSBERG'S THREE-PILLAR FRAMEWORK

The test centre supports a unified infrastructure protection model built on KONGSBERG's three operational pillars: Situational Awareness, Response & Inspection and Surveillance & Monitoring. Each pillar addresses a specific operational requirement – but they are designed to work together as a coordinated, modular system.

1. Situational Awareness: Building the operational picture

Effective protection begins with a clear understanding of what's happening both above and below the waterline. KONGSBERG's situational awareness systems aggregate data from multiple domains and sensor types, including:

- | Radar stations tracking vessel traffic around ports and coastal approaches.
- | Satellite-based AIS signals provided via KSAT, with global coverage including polar regions.
- | Seabed-deployed acoustic sensors monitoring structural activity and ambient noise.
- | Optical and SAR satellite imagery for surface-level verification.
- | Hydroacoustic and chemical sensors embedded along pipelines or power cables.
- | Environmental sensors carried by mobile Autonomous Underwater Vehicle (AUV) platforms.





Courtesy of Kongsberg

All inputs are processed using KONGSBERG's advanced sensor fusion and analytics platform, which integrates live and historical data to generate a shared situational picture. Machine learning models assist in identifying abnormal vessel behaviour, changes in seabed features or unusual patterns of activity around critical infrastructure.

Operators are not overwhelmed with raw data – instead, they access structured, role-specific interfaces designed to highlight deviations, recommend actions and support coordination between users. Features such as timeline reconstruction and mission replay further allow for post-event investigation, training and validation of incident response protocols.

As noted in recent European forums on undersea infrastructure security, operators and agencies across the region have emphasised the shortage of test environments that allow multi-sensor data to be integrated, validated and acted upon under operationally realistic conditions. The Oslofjord Test Bed is designed to close that gap.

2. Response & Inspection: From Detection to Confirmation

When a sensor alert or behavioural anomaly indicates a possible threat, rapid investigation is essential. KONGSBERG's inspection systems are deployed to confirm and characterise the event, using both autonomous and operator-guided platforms.

The core platform is the HUGIN AUV – widely recognised for its reliability and sensor versatility. Current configurations support:

- | Mission ranges exceeding 2,200 kilometres.
- | Operating depths of up to 6,000 metres.

- | Payloads including synthetic aperture sonar (SAS), multibeam echo sounders, magnetometers and high-resolution cameras.
- | Inertial navigation systems combined with DVL and GNSS surface correction.
- | Full support for autonomous mission execution or operator-directed tasks.

Alongside HUGIN, KONGSBERG also deploys ROVs for high-precision visual inspection and mechanical interaction – particularly in scenarios requiring manipulation, retrieval or verification in complex environments.

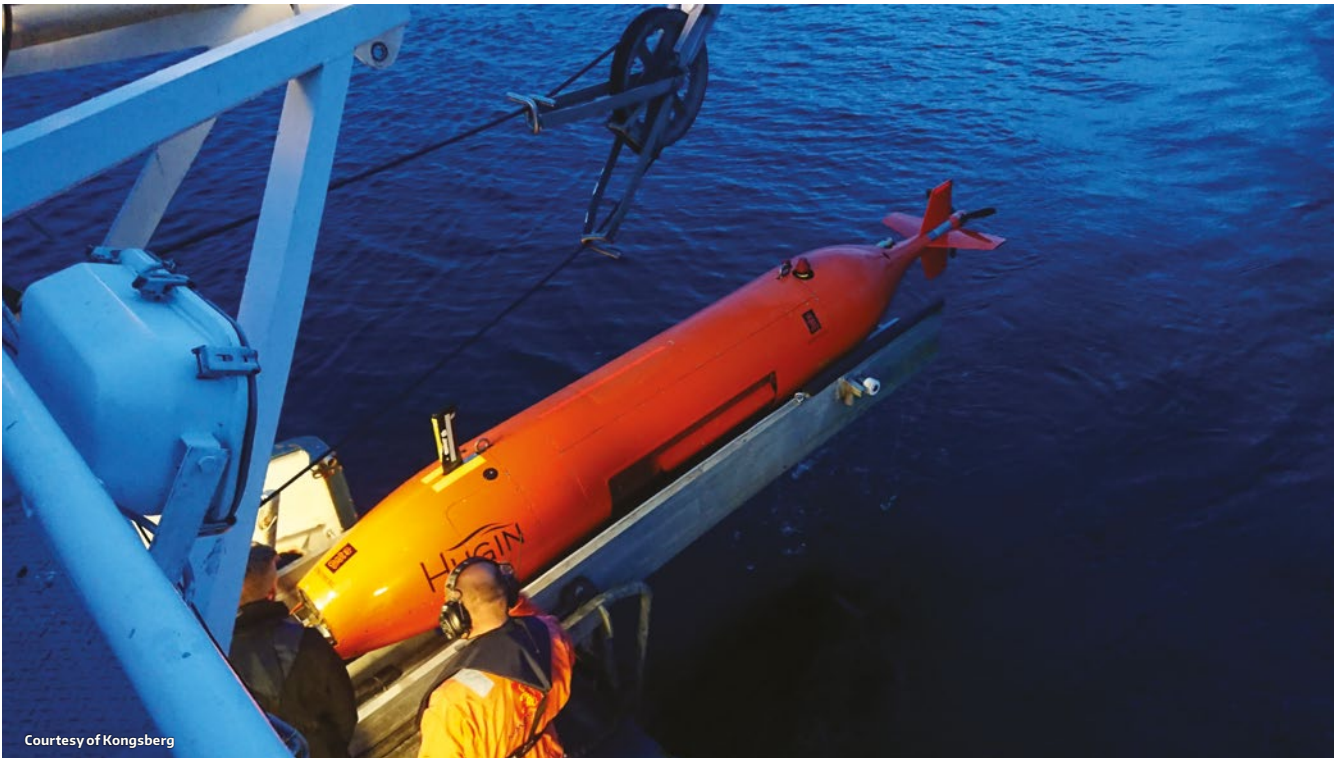
The Oslofjord Test Bed allows operators to simulate full inspection workflows: from anomaly detection to AUV tasking, data return and multi-platform coordination. These sequences are monitored, recorded and analysed in detail – supporting both technology refinement and human performance assessment.

3. Surveillance & Monitoring: Ensuring Long-Term Integrity

Beyond event-based response, the long-term integrity of infrastructure requires continuous or periodic monitoring. This is particularly important for subsea assets in remote or contested zones, where manual inspection is impractical or unsafe.

The test bed supports evaluation of persistent monitoring architectures, including:

- | Long-duration AUV patrols covering full pipeline or cable stretches.
- | Seabed acoustic nodes programmed for anomaly detection and satellite uplink.
- | Satellite-based change detection using radar imaging overlays.



Courtesy of Kongsberg

| Geofenced behavioural analysis tools that trigger alerts when vessels loiter or deviate from expected traffic lanes near sensitive areas.

One of the key technical objectives of the test bed is to improve change detection algorithms – helping systems distinguish between normal variation and actual threats, and to reduce false positives in noisy or high-traffic environments.

These systems are not just reactive. By comparing incoming sensor data to baseline surveys and incorporating long-term trend analysis, the platform supports predictive maintenance planning and infrastructure lifecycle optimisation.

STRATEGIC ALIGNMENT AND INTERNATIONAL COLLABORATION

The opening of the test bed follows clear policy signals from both national and EU institutions, as already stated. Norway's white paper on preparedness called for more extensive testing capabilities and cross-sector collaboration. The test bed has also been designed to support European Defence Fund (EDF) projects and other joint initiatives focused on infrastructure security and surveillance autonomy.

"The Oslofjord Test Bed provides a concrete tool to strengthen maritime preparedness," said Norwegian Minister of Energy Terje Aasland. "It shows how Norwegian technology and innovation can be applied to meet new threats and higher demands for security."

Håøy adds that "we believe maritime infrastructure is part of the foundation of democratic society – it supports how we power our homes, connect our economies and defend our freedoms. The Oslofjord facility is our commitment to that foundation: a place where public bodies, industry and technology meet to strengthen resilience where it matters most."

OUTLOOK: ENABLING INFORMED PROTECTION

As offshore energy systems expand, digital interconnectivity deepens and geopolitical risk increases, the need to protect CMI/ CUI is growing – both in scale and complexity. "There are many smart technologies in this space but very few environments where they can be tested together, under real conditions, by the people who will use them. That's the role we've created here. This is where integration becomes capability," Håøy emphasises.

Solutions will not come from individual technologies alone but from tested integration, operator preparedness and systems that deliver clarity in complex situations.

The Oslofjord test bed is not a showcase – it is a functional arena for engineering, learning and improving. By combining advanced autonomy, domain fusion, decision support and stakeholder engagement, it helps bridge the gap between today's threats and tomorrow's readiness.

"We see this not as a product centre but a preparedness platform," Håøy concludes. "It allows us and our partners to work with focus and precision on the systems that critical infrastructure protection urgently requires."



Maritime domain awareness

Know the now – **foresee** the next

DUAL-USE DILEMMA

HOW DUAL-USE TECH IS FUELING MILITARY THREATS BELOW THE SURFACE

Cathrine Lagerberg, Dual-use, Risk & Security Expert and Partner, InSilent AS

In July the *Baltic Sentinel* revealed that the new Russian Shahed drones – technically classified as autonomous unmanned aerial vehicles (UAV), – were powered by American Nvidia microchips.

NVIDIA Orin chips are dual-use classified items and require export licenses to restricted countries due to their military use potential. Yet despite export control and corporate compliance, these and other dual-use components continue to find their way to Russia. Why does that happen, and does it matter?

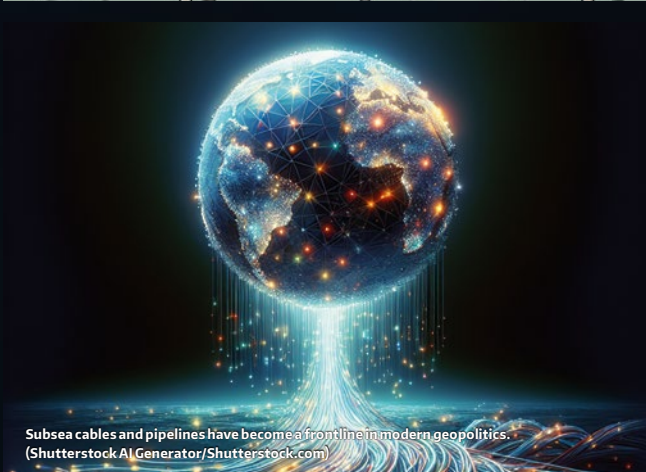
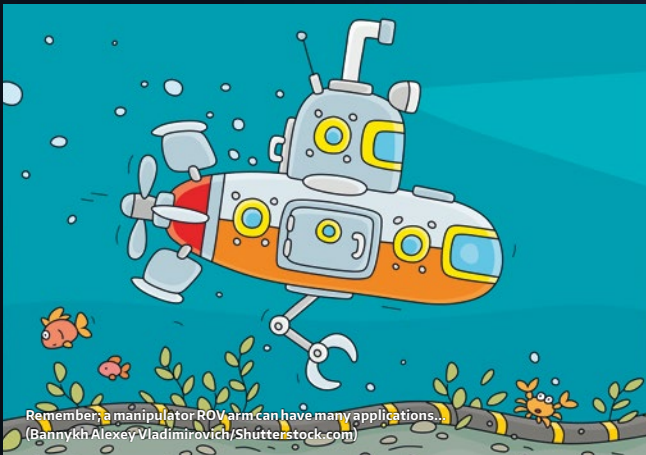
1) EXPORT CONTROL IS REACTIVE

Regulations are deemed to be circumvented because export control is reactive. But many forget that what we export can be used against us.

Take sonars and underwater instruments for instance. We know that both Russia and Chinese vessels are using Western underwater technology, remotely operated vehicles (ROVs), autonomous underwater vehicles (AUVs) and sensors. These are technologies that the west has excelled at producing.

Geopolitical tensions are increasingly playing out beneath the surface—along the very cables and pipelines that connect the world. (Vismar UK/Shutterstock.com)





Therefore, whether it is scientific vessels, luxury yachts owned by Russian oligarchs, or top modern fishing vessels, they are all equipped with western sensors and mapping instruments.

Despite increasingly comprehensive export control regimes and tougher sanctions, dual-use technologies like drones, sonar, and high-performance microelectronics are still reaching Russia.

2) CIRCUMVENTING EXPORT CONTROL IS OFTEN SIMPLE

Profit-driven actors, brokers, and intermediaries in third countries that are not sanctioned – like the UAE, Singapore, Turkey, and China – remain a regulatory export “grey zone”. Many companies know these countries are high risk and widely known to be used for circumvention, but they are not blacklisted nor illegal to sell to. Thus, they fall into the category of “problematic, suspected, tedious to screen, but not required and not prohibited to sell to”.

Furthermore, this level of complexity can increase depending on a country’s individual geopolitical circumstances. For example, Turkey being a member of NATO; China being an important trade partner. This makes sales versus skepticism a difficult part of international trade because this is also

politically sensitive and a matter of ongoing debates. As a result, exports pass through, screening is often avoided, and companies continue to sell. The consequences are also few, and where they do exist, they are minimal.

3) THIS EXPORT-CONTROL GAP POSES A GROWING RISK TO CRITICAL UNDER-WATER INFRASTRUCTURE (CUI)

The same technology needed for protection of subsea cables, pipelines, and other infrastructure underwater is also critical for detection, mapping, and targeting of the same systems.

Whether it's inertial navigation units, microelectronics, Doppler instruments, echo sounders, positioning and communication systems, ROV manipulators and tools, thickness gauges, sub-bottom profilers, or aerial drones: these are all dual-use items. All this technology can be as easily used to defend our infrastructure as it can be used to target it.

These components and instruments are needed by threat actors who want to identify our weaknesses, map coordinates and targets, and prepare for future operations like sabotage.

Many of these components are non-listed, commercially available, and often assessed by companies as “civilian, harmless, and not particularly dual-use”. Whether this reflects genuine ignorance or turning a blind eye is sometimes difficult to tell. But having spoken to many companies, one thing is clear: many are under pressure. They are striving to deliver and satisfy management and investors, and are simply required to prioritize profit over security.

4) EXPORT CONTROL SYSTEMS ARE BUREAUCRATIC, COMPLICATED, AND SLOW

Many larger defense and aerospace technology companies – the so-called primes – typically have liaisons and established connections to export control authorities and security services, dedicated compliance officers, lawyers and due-diligence expertise. At the same time, many small and medium sized companies do not have the same resources, situational awareness, or threat understanding.

As the global threat landscape evolves and sanctioned countries change and adapt their circumvention methods and third countries, one thing is certain: sanctioned and blacklisted entities and companies know that they are on the lists and avoid procuring directly through these.

Traditional export control screening processes often rely on outdated databases and remain reactive. In today’s threat landscape, legal compliance alone is not enough. Threat actors disregard laws and use whatever means necessary: false end-user certificates, shell companies, or illicit proxies.



Underwater cable system connecting countries and continents are critical to protect but easy targets. (Shutterstock AI/Shutterstock.com)

Therefore, extended risk assessments should be carried out beyond the purely legal requirements, in order to uncover connections and risks that conventional checks do not capture. A due diligence assessment may be sufficient under current legal frameworks, but in many cases traditional background checks fail to identify all of today's risks.

What's needed is therefore a more proactive and strategic approach where screening and background checks (integrity, enhanced and risk based due diligence) require much more sophisticated collection and analysis. They require companies to risk assess more broadly, and to include non-sanctioned but high-risk countries.

This is where private sector capabilities can complement the existing national export control bodies and traditional law firms assisting companies within sanctions and export control. By leveraging or investing in export, intelligence and screening consultants, either in-house or expert consultants, companies can not only remain compliant but conduct export checks and end-user verifications much quicker than most authorities and export control government bodies can.

Private companies can leverage company models that are less burdened by bureaucracy. They can also leverage technologically advanced OSINT platforms and AI collection tools, for much quicker and sometimes even more rigorous screening of people and companies. This allows for comprehensive, extensive, and high-resolution screening of companies and supply chains, without unnecessary delays or future reputational harm.

Some compliance departments have halted all export to Turkey out of fear of media coverage and future potential damage to company reputation if their components were to reach Russia via re-export and diversion. By conducting thorough risk assessments of distributors, supply chains, and end-uses, companies can reduce the export risk and conduct case-by-case assessments.

In short: modern, intelligence-led export compliance doesn't have to mean slower trade. It can mean smarter, faster, and more secure trade.

5) SECURITY CAN BE A COMPETITIVE ADVANTAGE

While export lists and licensing regimes evolve, illicit networks evolve faster, and circumvention is deemed likely. But as seen with Nvidia, media coverage can quickly escalate and cause severe reputational damage, impacting both public trust and company's stock prices and value.

Despite varying degrees of legal consequences across countries, Denmark recently announced significant tightening of criminal penalties and fines related to export violations. This included stricter jail sentences for executives who fail to conduct adequate screening. This reflects a shift where regulatory tolerance is narrowing, while expectations for proactive due diligence are increasing.

Given today's threat landscape, security and compliance are no longer just about checklists, compliance and regulatory obligations; they are part of allies' commitment, and a collective responsibility to protect shared critical CUI and security interests.

Modern export control must reflect the realities of geopolitics. The technologies used to protect CUI — sonars, drones, microelectronics, positioning systems, etc. — are the same technologies that adversaries seek to procure and use against us. Therefore, export control is no longer a desk office function. Rather, it's a front-line tool of strategic deterrence. As such, companies are our last line of defense.

Businesses that invest in proactive, intelligence-based export control can do more than just reduce risk. They can also build trust, contribute to allied resilience, and position themselves as committed actors in a world where certainty is becoming a scarce resource.

While the challenge in 'Baltic Sentry' is detecting interference with seabed CUI, understanding the threat requires layered, multidomain maritime situational awareness, underwater, on the surface, in the air, and in space. (Courtesy of NATO Maritime Command)



SURVEILLANCE NETWORK

NATO'S BALTIC SENTRY BUILDS CONNECTIONS TO COUNTER CUI THREAT

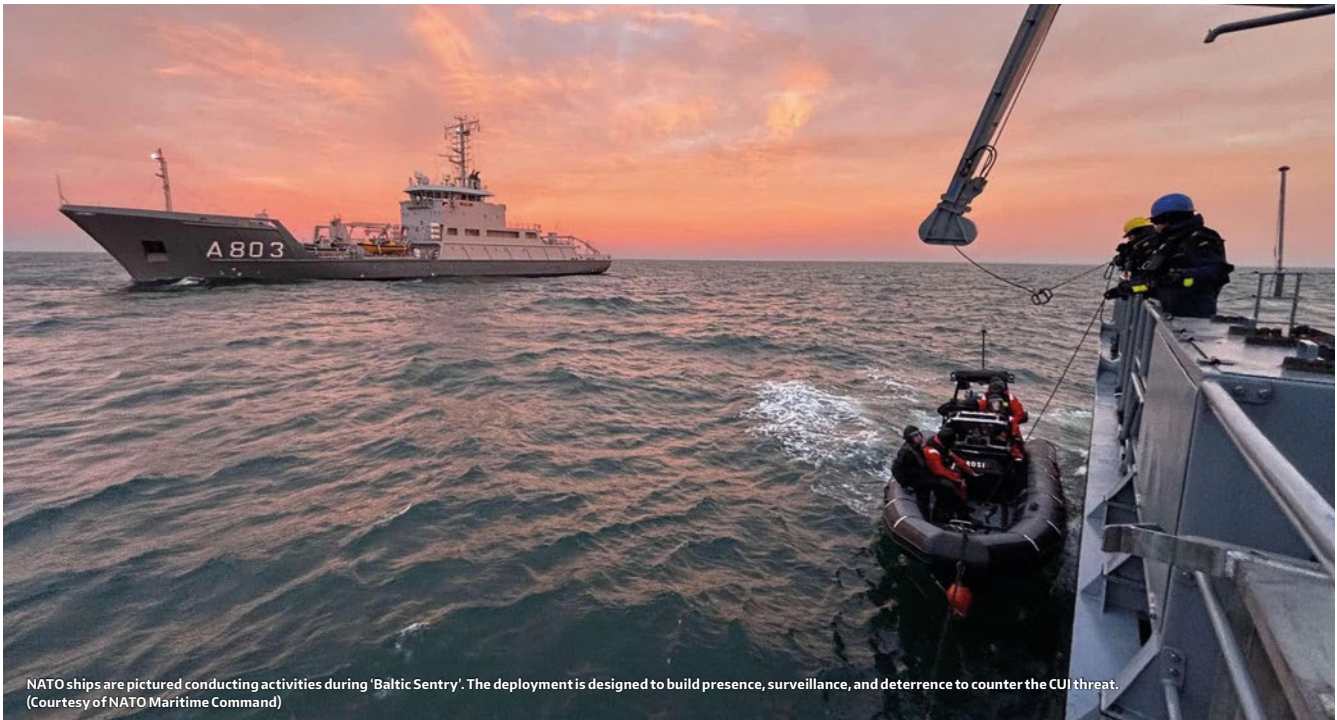
Dr Lee Willett

Since January 2025, NATO has been conducting its 'Baltic Sentry' maritime presence, surveillance, and deterrence activity in the Baltic Sea, responding to a series of incidents in which critical underwater infrastructure (CUI) was damaged. Since January 2025 and the establishment of 'Baltic Sentry', there have been no further reported incidents of malign actions against CUI. While it is difficult to prove the reason why something did not happen, one factor that may have had significant presence, surveillance, and deterrence impact is a vast network of strategic, operational, and information-based connections that NATO has built around 'Baltic Sentry'.



KONGSBERG

Real-time insights
for **rapid response**



NATO's network of connections includes: key NATO allies across and outside the region; senior NATO operational commands and decision makers; maritime operations centres (MOCs), both national and multinational (the latter including NATO Allied Maritime Command [MARCOM] in the UK as the operational command 'hub', and Commander Task Force Baltic [CTFB] in Germany); and operational units at sea, including NATO and national assets.

Other network 'nodes' located in and around MARCOM itself, at the UK's Northwood headquarters, include the NATO Shipping Centre and the NATO Maritime Centre for the Security of CUI (NMCSCUI). The latter is NATO's CUI stakeholder operational co-ordination cell, the operational-level counterpart of the Brussels-located CUI Co-ordination Cell (CUICC) that provides strategic-level stakeholder co-ordination.

Demonstrating that dealing with the CUI threat is a multi-domain task, requiring layered, integrated surveillance and response capacity, the operational units at sea have another 'network' built around them. Operational and tactical level output is based around the 'hub' of two NATO task groups, Standing NATO Maritime Group 1 and Standing NATO Mine Counter Measures Group 1. Around this at-sea 'hub' are layered connections from the seabed to space, including: seabed sensors and uncrewed underwater vehicles (UUVs) below the surface; surface ships and support ships on the surface (with occasional additional presence from uncrewed surface vessels [USVs] being trialled by NATO Allied Command Transformation's Task Force X Baltic programme, alongside but not part of 'Baltic Sentry' activities); maritime patrol aircraft and uncrewed aerial vehicles (UAVs) in the air; and satellite sensors in space.

Such assets are operated by NATO or by individual alliance member states. However, all are integrated together, bringing surveillance and response presence to build deterrence against the risk.

THE RISK

The Baltic Sea has been something of a case study in the rise of the global risk to CUI, in the context of the development of 'grey zone', asymmetric, hybrid activities in and around areas of crisis and conflict. Against the backdrop of the Russo-Ukraine war accelerating through mid-2022 (following its outbreak in February that year), in September 2022 two Nordstream gas pipelines off Denmark's Bornholm island in the Baltic were ruptured by explosions. This incident put the CUI risk firmly at the centre of the global politico-strategic spotlight.

Next, between October 2023 and December 2024, three separate incidents occurred in the Baltic, in which gas pipelines and data and power cables were damaged by commercial ships allegedly dragging their anchors across the seabed.

What followed was significant political and public debate across northern Europe, regarding whether the ships were 'shadow fleet vessels' – vessels that support various malign activities on behalf of rogue states.

THE RESPONSE

While this debate continued, 'Baltic Sentry' was stood up at sea, and various NATO and national commands began work ashore to connect up strategic- and operational-level stakeholders to knit together a surveillance and decision-making network wide enough and deep enough to deter the threat, through enhancing awareness and understanding of the surface and sub-surface domains together, and through generating capacity to respond rapidly to any threat.



This network – and the required steps and procedures introduced to enable it to function effectively – enables stakeholders to communicate daily, including sharing information and intelligence in near real time, to support operational- and tactical-level direction and co-ordination so as to expedite response time of 'Baltic Sentry' units at sea, Commander Arlo Abrahamson, MARCOM's chief spokesperson, told Ocean Robotics Planet.

"The reason we're able to respond quickly is because, over a number of months, the alliance has been able to strengthen its network, not only in the Baltic countries but other allied countries that have contributed," Cdr Abrahamson explained. "We know about [incidents] quicker and we understand the environment better, and we're able to respond much faster because we've built this network."

The urgency of the requirement to respond to the risk and the importance placed by allies on securing CUI drove the establishment of this network as the central node of NATO's response, Cdr Abrahamson explained. "It is the core that allows us to deter and have assets in place, respond quickly, and then if necessary, after the response decide if an incident requires an investigation."

This network is not a tactical communications network. NATO has a long-established structure of technological routes through which navies communicate at a tactical level. Instead, this particular network is about stakeholder engagement.

"I'm talking about the relationships, the allies being familiar with each other on these specific issues," said Cdr

Abrahamson. "When you have to communicate frequently on specific issues related to CUI to help understand the environment, that is the network that has become much stronger because of 'Baltic Sentry'."

The importance of this network mirrors, and is driven by, the importance NATO places not only on CUI security but on the wider flow of commerce along other strategic-level sea lines of communication that dissect the Baltic Sea and connect it to regions beyond. To support these and wider NATO security interests, the alliance established – in the years preceding the Russo-Ukraine war, as instability increased – enhanced vigilance activity (EVA) presence in key regions across the Euro-Atlantic theatre. The Baltic is one such region, and 'Baltic Sentry' is feeding into and supporting the EVA requirement there.

"The vision for 'Baltic Sentry' is about sustaining the ability for NATO to have this network and to have sustained presence," said Cdr Abrahamson. Such sustained presence is essential for NATO in building deterrence plus expedience and capacity in response to any suspicious activity. "Where there's activity occurring that's of interest to allies, our ability to share information, co-ordinate, and respond is better than it's ever been, and that's partly due to the strong networks built around 'Baltic Sentry,'" Cdr Abrahamson added.

Going forward, Cdr Abrahamson continued, NATO sees an increased role for NMCS CUI and CTFB as key co-ordination nodes for allied protection of CUI.



Ocean Robotics
Planet



**CRITICAL UNDERSEA
INFRASTRUCTURE PROTECTION**

SPECIAL REPORT

Supported by



KONGSBERG