

# Ocean Robotics Planet

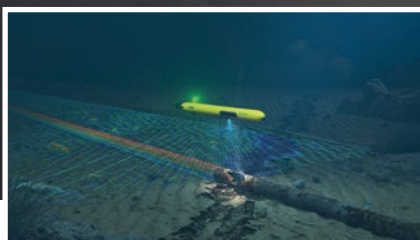
Supported by

 **TELEDYNE** | Marine

## CRITICAL UNDERSEA INFRASTRUCTURE PROTECTION

CUI

**SPECIAL REPORT**



2. CUI Protection: Remote Sensing Solutions for Underwater Assurance



6. Norway's CUI Security Approach Illustrates Combined Industry/Navy Role in Multi-stakeholder Co-operation



9. How USV-AUV Mothership Operations Are Redefining Protection of Critical Underwater Infrastructure

# CUI PROTECTION

# REMOTE SENSING SOLUTIONS FOR UNDERWATER ASSURANCE

By Ed Cheesman, Business Development Director, Teledyne Marine

---

**Critical Underwater Infrastructure.** Until recently not a topic that kept many of us awake at night. Being distant and out of sight, one might have been forgiven until lately for taking little interest in the network of cables and pipelines that criss-cross our seabeds. However, these unseen assets are at risk and in a way that is leading to insomnia for more than just the host of structural and integrity engineers who design and manage these impressive underwater networks.

---

Forming the backbone of modern global economies, carrying critical data, delivering essential hydrocarbons for industry and facilitating the flow of electricity from production to point of use, these subsea assets have key vulnerabilities. And while the ocean environment itself can be unforgiving to underwater infrastructure, it is not only natural forces or accidental damage that need to concern us these days.

## EMERGING THREATS TO UNDERSEA NETWORKS

A cursory glance in the media quickly reveals a host of articles concerning foreign “spy ships” and “ghost vessels” loitering uncomfortably close to our critical cables, pipelines, and offshore installations prompting concern that such ships may be planning hostile, damaging and disruptive acts toward these critical assets if not today, then at some future hour.



The UK's multi-role ocean surveillance ship RFA Proteus stays close to Russian 'spy' ship Yantar in the Irish Sea in November sending clear signal, "We see you!"

Meanwhile an increase in seemingly 'accidental' incidents particularly centred around the Baltic Sea where cables are being damaged and even severed by ships dragging their anchors across their path has attracted much media attention. Since October 2023, no fewer than 11 submarine cables have been cut in the Baltic Sea in a series of suspect incidents with a number of others damaged. As recently as New Year's Eve 2025, the Finnish police seized a cargo vessel on suspicion of sabotaging an undersea telecoms cable running from Helsinki across the Gulf of Finland to Estonia, this following a similar incident in the same area on Christmas Day 2024.

As nations grapple, no pun intended, with what is to be done to prevent such criminal damage, governments are increasingly turning to industry for solutions.

### DETECTING DANGER ABOVE AND BELOW THE WAVES

Of particular interest are technologies to help detect potential threats before an incident occurs, in the hope that those responsible for guarding the assets may be able to prevent an incident or attack. Equally important are solutions for mapping damage following an incident allowing authorities to piece together the sequence of events which led to any subsequent damage.



Capable of deploying subsea submersibles, Yantar is operated by the Russian Directorate of Deep-Sea Research (GUGI)

information is essential for assigning attribution and can prove to be vital evidence in any criminal damage cases which may follow. Having attributed and where possible warned an offending party of the danger posed by their actions there can be no plausible deniability.

Securing these underwater networks against threats requires a combined approach.

Above the waves, AIS (Automatic Identification Systems), plays a significant part in any surveillance solution and allows for monitoring routine vessel traffic operating in the area. As vessels can deliberately switch off their AIS however, or broadcast false information, it is important to ground-truth this information by augmenting it with radar data and camera footage to give a more complete picture above the water and of course also in the air. These specialised cameras use electro-optical (EO) for daytime and infra-red (IR) for night vision and come equipped with powerful continuous-zoom telescopes which help detect, identify and track targets from great distances.

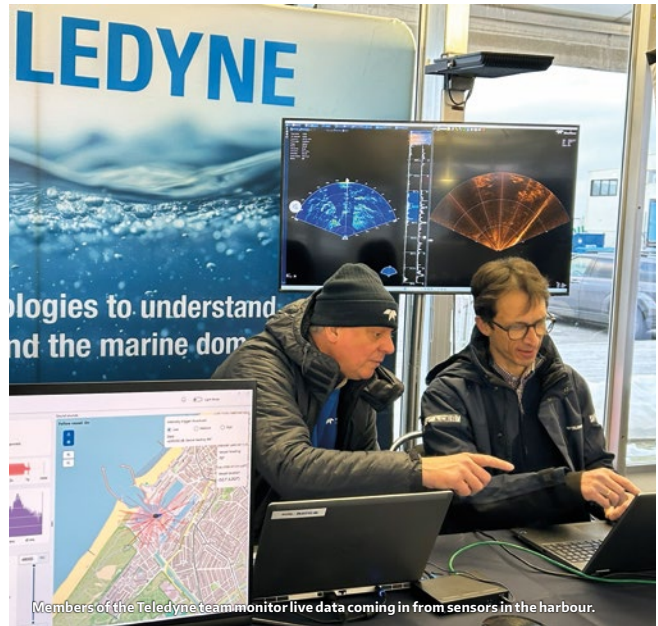
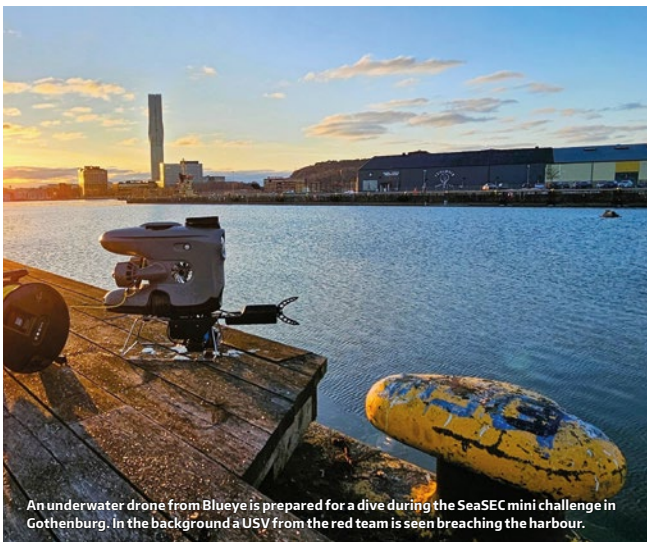
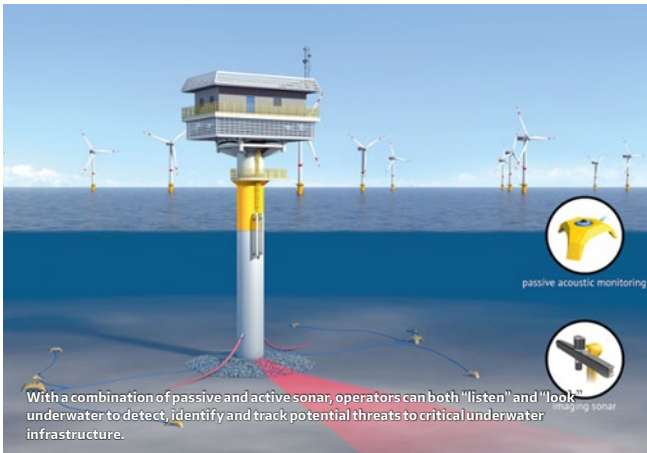
Meantime below the water, where visibility is much more limited, passive and active sonar techniques can be used to monitor for unusual activity close to or approaching toward



Finnish police seize a cargo vessel, on suspicion of sabotaging an undersea telecoms cable running from Helsinki across the Gulf of Finland to Estonia (Lehtikuva/Finnish-Police)

Delivering technology to detect, monitor & secure vital systems





Passive Acoustic Monitoring (PAM) uses hydrophones (underwater microphones) to record ambient sounds in aquatic environments. Using advanced processing techniques, PAM systems can be tuned to filter out background noise and listen in to specific sounds of interest. These might include the sound of an anchor dragging, the acoustic chirp from an underwater vehicle mapping the seabed or sounds emitted from a diver in the water.

Similarly, forward looking sonar (FLS) systems, a type of active sonar analogous to a video camera, can also prove an effective tool for visualising underwater activity.

FLS systems can be networked together and used to continuously monitor specific locations e.g giving real-time surveillance around a localised asset or chokepoint, much like having an underwater network of CCTV cameras. Alternatively these “acoustic” cameras can sit silently waiting to be triggered on detection of specific signatures detected by the PAM system.

Either way, a combination of passive and active sonar makes for a robust and effective means of creating a tactical picture below the waves where visibility is often limited and optical cameras are of little practical use due to a combination of factors including high turbidity and their

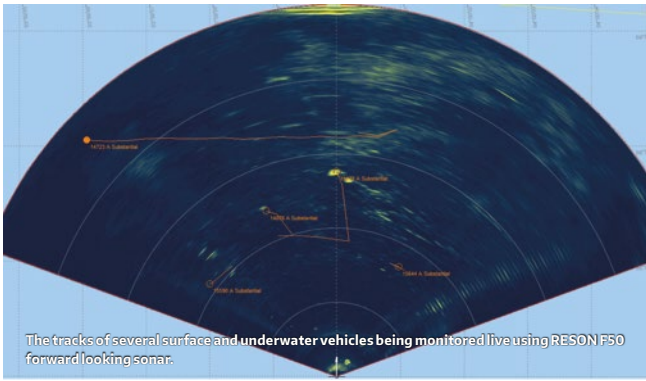
limited range. Such sonar systems ensure early detection of suspicious activities and with the right alarming logic programmed in, can prove a useful means of identifying potential threats.

### TURNING DATA INTO ACTIONABLE INTELLIGENCE

Whether coming from above or below the water, such data is typically fed to a command and control software (or “C2” system), which fuses together all available information. This gives not just real time situational awareness but a complete tactical picture providing actionable data for any potential threat response.

Such solutions are of commonplace in military settings but are a bit of a step change for security operations in the offshore telecoms, energy or utility sectors.

This makes operational exercises like SeaSEC (Sea Security) really important. SeaSEC is a unique multinational initiative designed to strengthen the protection of critical seabed infrastructure. Operating under the Northern Naval Capability Cooperation (NNCC), SeaSEC brings together military and government organisations from allied nations with asset owners and industry players in order to co-develop and validate innovative solutions.



On February 2nd 2026 during the annual Navy Tech event in Gothenburg, SeaSEC organised a mini harbour challenge event to put some of these industrial solutions to the test. Pitting a blue team, comprising of industry, against simulated red team intruders, comprising of unmanned surface vessels, ROVs and AUVs, participants were challenged to conduct real time detection of simulated threats.

Teledyne demonstrated how PAM systems using RESON's reference grade hydrophones can be used to display and visualise vital information such as target identification, course and track of potential threats and how, where processed in real-time, such tracks can be streamed live to C2 systems providing relevant, actionable information.

Teledyne also demonstrated how multi-sensor approaches can strengthen harbour defence. As part of the live demonstration two forward looking sonars, namely the SeaBat F50 from RESON and the BlueView M900/2250 were collocated on a subsea frame which was lowered to the harbour floor. These gave a clear, real-time view of underwater activity in the busy harbour environment.

Meantime a FLIR Ranger HDC EO/IR camera mounted quayside gave continuous surveillance above the waterline staying vigilant to any surface and airborne threats.



This combination proved effective and highlighted just how challenging it can be for a would-be saboteur to remain undetected in such a well monitored harbour setting. However, there is work yet to do. It is one thing to demonstrate capability and another to roll it out.

Industrial partners can play their part to develop solutions but it is for governments to act: deciding who is responsible, which assets are most vital to protect and as ever, who should pay for this peace of mind. Until then, for some at least, there may yet be some sleepless nights.

Norway is home to an extensive CUI network offshore, which it secures through a co-operative relationship between the government, maritime agencies, armed forces, and industry. (Courtesy of Norwegian Armed Forces)



# WIN, WIN

## NORWAY'S CUI SECURITY APPROACH ILLUSTRATES COMBINED INDUSTRY/NAVY ROLE IN MULTI-STAKEHOLDER CO-OPERATION

Dr Lee Willett

Norway has perhaps a unique geostrategic perspective on the threat to critical underwater infrastructure (CUI) within NATO's area of responsibility.

First, it has an extensive national CUI network – mostly offshore oil and gas, but also power and data cables – through which it shares its resources with NATO allies and other international partners.

Second, this extensive network reflects the fact that Norway is home to commercial industry that holds significant expertise, capability, and capacity in building, operating, and maintaining such a network. Such capability and capacity include maritime uncrewed systems in the surface and – especially – sub-surface domains.

Third, Norway has experienced suspected CUI attacks – and prior to the CUI threat surfacing in European political and public consciousness following the Baltic Sea Nordstream gas pipeline explosions in September 2022, data cables connecting the SvalSat satellite station on Norway's Svalbard Island to the mainland reportedly were cut. In November 2021, several kilometres of sensor cable were reported to have been torn from a civilian-run environmental monitoring network off the Lofoten peninsula, on the northern stretches of Norway's mainland. These incidents occurred at either end of the Bear Gap, which divides the relatively shallow waters of the Barents Sea from the deeper Norwegian Sea and is a key transit area for underwater traffic.



Norway works with international partners to deter CUI threats. The Royal Norwegian Navy (RNoN) frigate HNoMS Fridtjof Nansen (left) is pictured bringing maritime situational awareness presence at the Goliat oil field, during a UK-led Joint Expeditionary Force deployment. (Courtesy of Norwegian Armed Forces)

Norway’s geostrategic position is thus significant when considering CUI threats. Its CUI security capacity, capability, and experience are significant, too.

It was thus unsurprising that, in the immediate post-Nordstream period, Norway led an international response including Denmark, Germany, the Netherlands, and the UK to survey almost 9,000 kilometres of pipelines and cables across the five countries’ national sectors. A crucial component of this collaboration was the ability to tap into the Norwegian commercial marine industrial sector’s collective pool of over 600 uncrewed underwater vehicles (UUVs).

### NATIONAL POWER

Norway itself has 8,800 km of oil and gas pipelines offshore, which supplied Europe with 30 percent of its gas in 2024. The country also hosts 400 electric power plants, which are connected by seabed power cables to Denmark, Germany, and the UK. It also has, of course, fibre-optic data cables.

“This infrastructure is owned by industry, it is established by industry, and it is put on the seabed by industry. It is inspected and monitored by industry. If it is broken, it is repaired by industry,” Commodore Kyrre Haugen – Commander Norwegian Fleet for the Royal Norwegian Navy (RNoN) – told the DefenceIQ ‘Seabed Security’ conference in Tróia, Portugal in September 2025.

“The true muscle is within industry, with hundreds of remotely operated vehicles (ROVs) and other systems available for pipeline and cable surveillance. This provides resilience,” said Cdre Haugen.

“The subsea industry in Norway is ... world class. They find sensible solutions to different problem sets,” the Cdre continued. Industry has been establishing and surveying its

own integrated seabed infrastructure for decades, and the system has some in-built redundancy for when maintenance is required or accidental damage occurs; industry also holds data that is available for the armed forces, he added.

Today, given the CUI threat’s increasingly urgent nature, Norway’s commercial industry conducts risk analysis with an emphasis on security alongside safety, Cdre Haugen explained. There is recognition amongst the different stakeholders including industry and the military that common situational understanding is required to help the government and armed forces protect what may need to be protected.

In the current security context, protecting CUI involves multi-stakeholder co-operation due to the possibility of seabed interference by various outside actors. For example, three incidents of CUI damage in the Baltic Sea that occurred between October 2023 and December 2024 prompted questions within the NATO community of whether such damage was caused by commercial ships purposefully dragging their anchors across the seabed for extended distances.

A co-operative approach to CUI security involves commercial industry, various governmental departments and agencies, maritime police and other marine authorities, and the armed forces – especially navies.

“There is a naval role in deterring the CUI threat: we have responsibility for maritime situational awareness (MSA),” Cdre Haugen said. More broadly, the armed forces provide further support and co-ordination in securing CUI, he added.

The Norwegian experience illustrates its multi-agency approach, in particular sharing information across different stakeholders.





Norway's co-operation approach encompasses equipment capability development. Here, the RNoN deploys a Hugin AUV from a Norwegian Coast Guard vessel. (Courtesy of Norwegian Armed Forces)

“Deterring, defending against, and responding to CUI threats is all about using available information,” said Cdre Haugen. “Connecting the coastguard, the fleet, customs, the police, maritime authorities, and the major industry players together by sharing information from different sources is the key to being able to monitor such a wide and broad network of pipelines and cables, and a huge variety of different areas.”

Norway has taken specific steps to ingrain such co-operation deeply into its CUI security processes. “We have established a maritime security network with key stakeholders gathered on a regular basis, discussing relevant topics and doing tabletop exercises,” said Cdre Haugen. “Industry’s key elements have their own operational centres with classified facilities: these are in regular connection and communication with the naval Maritime Operations Centre – sharing information, and accessing information they need.”

### CO-OPERATIVE INNOVATION

Norway’s industrial and naval operators are also innovating to improve CUI security capacity.

Industry’s innovation in uncrewed systems, sensors, data, and artificial intelligence is impressive, said Cdre Haugen.

Moreover, industry is developing a significant network and capacity to improve efficiency and agility in CUI surveillance not only to reduce risk of network disruption impacting availability of industry’s service but because of the national focus on keeping CUI secure, Cdre Haugen explained. “That’s a win-win situation,” he added.

Collaborative steps have also been taken to make better use of available information. For example, sensors used by the commercial companies to monitor their systems’ safety are now increasingly integrated into Norway’s wider information-sharing network to enable MSA to be further enhanced. Physically connecting such sensing capacity into the wider national network also provides an appropriate means of sharing classified CUI information, Cdre Haugen explained.

As regards the RNoN’s own capacity development, Cdre Haugen highlighted the navy’s investment in UUVs for CUI surveillance and threat detection. For example, he explained, “The RNoN has improved its ocean-going autonomous underwater vehicle (AUV) capabilities, using a container-based system that can be deployed from several ships in the fleet.”

The RNoN also uses its mine countermeasures expertise including mine clearance divers to support industry CUI surveillance needs, he added.

In CUI surveillance terms, the military requirement differs slightly from that of industry. Industry needs to surveil its entire network to ensure it all works. From the military perspective, Cdre Haugen explained, “There are other objects out there and cables at the bottom that we are more focused on to survey and protect. This is part of the risk analysis, because not all CUI is vulnerable or vital to protect as there is a lot of redundancy in the system.” “So, by analysing and conducting risk assessments, we identify ‘hot spots’ in the network and keep focusing on those,” the Cdre added.

# ALWAYS ONE AUV IN THE WATER

## HOW USV-AUV MOTHERSHIP OPERATIONS ARE REDEFINING PROTECTION OF CRITICAL UNDERWATER INFRASTRUCTURE

By Thomas Meurling

**Critical Underwater Infrastructure (CUI), subsea pipelines, power cables, and global communications links form the invisible foundation of modern society. These assets that carry energy, data, and provide economic stability across oceans are quietly enabling everything from national defense to daily digital life, whilst also becoming increasingly vulnerable.**

The sabotage of the Nord Stream pipelines in 2022 and the damage to the Baltic pipeline in 2023 did more than disrupt energy flows. These incidents revealed that much of the critical seabed infrastructure remains unprotected, insufficiently monitored, and difficult to defend via traditional maritime surveillance.

What makes the challenge even more complex is the nature of the threat. Many hostile actions targeting CUI fall into the “grey zone”. Though deliberate and deniable, they’re intended to avert escalation whilst still achieving strategic effects. Attribution is difficult, deterrence even harder, and episodic monitoring is no longer enough. Protecting CUI now requires persistent, high-resolution, and cost-effective underwater surveillance on a continuous basis.

### WHY TRADITIONAL SURVEILLANCE MODELS FALL SHORT

Established approaches to subsea monitoring struggle to meet this requirement. Fixed seabed systems, such as hydrophone arrays, provide persistent monitoring but only at known locations. Once identified, they can be avoided, spoofed, or neutralised. Their static nature is both an advantage and a limitation.

Crewed vessels deliver mobility, but at a prohibitive cost. Daily operating expenses routinely exceed tens or hundreds of thousands of dollars. Their acoustic and visual signatures are unmistakable, making discreet monitoring impossible. Most critically, launching and recovering underwater systems in real sea states exposes crews and equipment to considerable risk.

Standalone AUV operations solve some problems, but cause another: endurance. Battery limitations typically restrict missions to less than 24 hours. When depleted, the AUV must be recovered, recharged, and redeployed. The result is a stop-start surveillance model, punctuated by gaps precisely when persistence matters most.

In short, today’s tools were never designed for continuous, wide-area CUI protection.



## PERSISTENT UNDERWATER SURVEILLANCE: FROM 'WE CHECKED' TO 'WE ARE WATCHING'.

Courtesy of Thomas Meurling

### PERSISTENT SURVEILLANCE ARCHITECTURE

- MOBILE OPERATIONS HUB**  
USV as a forward-deployed command and control center.
- ONBOARD CHARGING & DATA TRANSFER**  
Refueling, data download, and diagnostics occur on the USV.
- MULTI-VEHICLE PLANNING**  
Smarter mission allocation, minimizing dead time and overlap.
- CONTINUOUS PRESENCE**  
Shifts from episodic surveys to constant monitoring.

**FOUR AUVs, ONE USV: ZERO BLIND TIME**

RESERVE/TRANSIT

**AUV 1: ON-MISSION**  
Actively surveying the infrastructure.

**AUV 2: CHARGING/HEALTH CHECK**  
Refueling and diagnostics.

**AUV 3: DATA OFFLOAD**  
Transferring mission data to the USV.

**AUV 4: RESERVE**  
Ready to deploy immediately.

**OPTIMIZED ROTATION FOR 24/7 COVERAGE**

### FROM "WE CHECKED LAST WEEK" TO "WE NEVER STOPPED WATCHING"

**OLD MODEL**

EPISODIC SURVEYS  
Blind for 80-90% of time. Vulnerable to threats between windows.

**NEW MODEL (PERSISTENT)**

CONTINUOUS SURVEILLANCE  
Constant seabed monitoring. Proactive threat detection.

**KEY BENEFITS**

- RESILIENCE**  
System adapts to failures and environmental conditions.
- EFFICIENCY**  
Automated operations and distributed energy.
- SECURITY**  
Real-time protection for critical infrastructure.

**STRATEGIC PING NEWSLETTER: Building a CONOPS-driven architecture for the future of seabed security**

### THE SHIFT: USVS AS MOTHERSHIPS, AUVS AS PERSISTENT SENSORS

A new operational model is emerging that fundamentally changes how subsea infrastructure can be protected.

At its core is a symbiotic USV-AUV concept: Unmanned Surface Vehicles acting as autonomous motherships, supporting and sustaining fleets of Autonomous Underwater Vehicles.

This does not concern replacing ships with drones. It is about breaking the endurance barrier and creating a system where at least one AUV is always in the water – surveying, mapping, and monitoring critical infrastructure – while others recharge, upload data, or stand by. Persistence becomes the standard, not the exception.

### THE OPERATIONAL PRINCIPLE: CONTINUOUS AUV ROTATION

The model is simple yet operationally effective. A USV deploys a fully charged AUV to survey a defined CUI corridor. As that AUV approaches its battery or mission limit, it autonomously returns to the USV. A launch-and-recovery system (LARS) enables safe, automated docking, often without the AUV even leaving the water. While the returning vehicle recharges and offloads data, a second AUV is deployed immediately.

The result is a continuous rotation cycle: 1 – one AUV surveying; 2 – one AUV charging; 3 – one AUV processing or standing by. There are no surveillance gaps, no need for

crewed recovery, and no dependence on weather windows to dictate operational tempo. This capability establishes the USV as an effective force-multiplying mothership.

### WHY MULTI-AUV LARS IS THE ENABLER

The most critical function of the USV in this architecture is launch and recovery, rather than navigation or endurance. A multi-AUV LARS transforms the USV from a basic platform into an autonomous subsea operations hub. It enables safe handling of multiple AUVs in real sea states; in-water docking for charging and data transfer; and elimination of deck-based recovery, the riskiest phase of any subsea mission.

Removing personnel from launch and recovery operations significantly increases safety. Meanwhile keeping AUVs submerged during servicing further increases operational uptime. In this case persistence is no longer limited by weather, daylight, or crew availability.

### AUVS: HIGH-RESOLUTION EYES ON THE SEABED

In this model, the AUV serves as the primary sensor platform, operating directly where CUI is located. Medium-class AUVs offer an optimal balance of payload capacity, endurance, and autonomy for monitoring infrastructure. Equipped with high-resolution sonar, such as Synthetic Aperture Sonar (SAS), they deliver centimeter-scale imagery across wide areas of the seabed. This level of resolution is essential, not optional.

It enables detection of subtle seabed disturbances, newly introduced objects, cable exposure, or burial changes, and provides evidence of tampering or pre-positioned devices. Importantly, it also enables repeatable and comparable surveys, supporting accurate pattern-of-life analysis along critical routes.

### FROM SEABED TO SHORE: TURNING DATA INTO DECISIONS

Persistence alone is insufficient; data must be transferred securely and efficiently. In the USV-AUV model, data flows seamlessly: 1 – raw sonar data is collected by the AUV; 2 – data is transferred during docking to the USV; 3 – data is then pre-processed onboard to flag anomalies and reduce bandwidth; 4 – pre-processed data is transmitted via encrypted satellite links to shore-based command centres.

The USV acts as a mobile data gateway, providing near-real-time intelligence to national or alliance-level command systems. Once integrated into a wider Maritime Domain Awareness framework, this continuous data stream enables a shift from reactive response to proactive infrastructure defense.

### STRATEGIC ADVANTAGES THAT REDEFINE THE MISSION

The benefits of this symbiotic model are transformational, not incremental.

| **PERSISTENCE AT SCALE:** Weeks or months of uninterrupted monitoring replace short, disconnected missions;

| **REDUCED RISK:** No crews are exposed to hazardous launch and recovery operations;

| **OPERATIONAL DISCRETION:** Low-profile USVs and submerged AUVs significantly reduce detectability;

| **ECONOMIC VIABILITY:** Replacing crewed support vessels with autonomous motherships makes persistent surveillance financially viable;

| **SCALABILITY:** Multiple USV-AUV teams can be deployed simultaneously throughout vast infrastructure networks.

Together, these advantages make unmanned systems a significant force multiplier for CUI protection.

### A NEW DOCTRINE FOR UNDERWATER SECURITY

The protection of Critical Underwater Infrastructure is no longer a niche technical problem, it's a strategic requirement. The USV-AUV mothership model offers a forward-looking doctrine – one designed for endurance, ambiguity, and scale. By making sure that there is always an AUV in the water, it delivers the persistence required to deter, detect, and document hostile activity in the subsea domain.

While this model is highly relevant for CUI, its implications reach further to mine countermeasures, ISR, and long-term seabed monitoring. At a time when underwater infrastructure has become both a target and a strategic lever, adopting persistent, unmanned, and integrated surveillance architectures is no longer optional. It's the new baseline for maritime security.





# Ocean Robotics Planet



**CRITICAL UNDERSEA  
INFRASTRUCTURE PROTECTION**

**SPECIAL REPORT**

Supported by

 **TELEDYNE** | Marine