Exploiting the **underwater battlespace**

Building a subsea threat response

Digital Intelligence

BAE SYSTEMS

Introduction

The subsea domain is continuing to become increasingly contested, congested and complex. As such, the threat to nations is growing - both in terms of frequency and severity.

To quote from a recent Policy Exchange paper, "**From Seabed to Space**", released in 2024: "Technological and operational developments have brought geopolitical competition to the seabed. As the ability to manoeuvre, map and operate at greater depths increases, critical maritime infrastructure along the seabed resembles the exposed underbelly of national security in a new age of undersea warfare."

Clearly, the threat is significant and concerning. While undersea warfare is nothing new, recent incidents have served as a wake-up call regarding the growing threat to critical infrastructure on the seabed and the resulting risk to national security.

For example, in November 2024 two fibre-optic cables running under the Baltic Sea from Germany to Finland and Sweden to Lithuania were severed, followed by Estonia's power supply being significantly impacted when the main undersea electricity cable linking Finland with Estonia was damaged. These incidents **highlighted the Baltic region's status** as a global centre for suspected subsea infrastructure sabotage at a time of heightened geo-political tensions, prompting **NATO to launch a new mission** called "Baltic Sentry", increasing surveillance of ships in the Baltic Sea with aircraft, warships and drones.

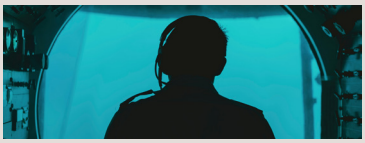
The issue was also highlighted in the **UK government's 2025 Strategic Defence Review**, which highlighted maritime security as a "strategic imperative for the UK" and referenced the Royal Navy's 'Atlantic Bastion' plan to "secure the North Atlantic for the UK and NATO against the persistent and growing underwater threat".

One of the key challenges facing governments is that the maritime threat is evolving beyond traditional domains to incorporate more grey-zone, sub-threshold tactics and strategies as necessary vehicles for delivering effect and maintaining the competitive edge.

> Threat levels are increasing, a wider group of sophisticated adversaries are emerging, and **the pace of change is only expected to accelerate**

Characterising the threat

Three capability areas are becoming ever more important due to the increasing subsea threat:



Intelligence, Surveillance and Reconnaissance (ISR)

Anti-Submarine Warfare (ASW)

Critical Undersea Infrastructure Protection (CUIP)

Not only are governments and commercial operators seeing an exponential increase in threats in these key areas, but they are facing the realisation that traditional capabilities and countermeasures are becoming less relevant and effective.

In ISR, the risk appetite to deploy a crewed submarine to conduct up-threat tasking is low, and in certain operational scenarios, not possible. Yet the need to gain intelligence early from strategically positioned indicators and warnings that give a competitive advantage over adversaries in the underwater domain, is only increasing.

Similarly, the demand for information and intelligence to inform timely decision-making to counter the ASW threat in multiple regions, simultaneously and persistently, is significant. In fact, the sheer scale of this challenge outmatches many nations' current force structures.

Overlaid on these threat vectors is the growing risk to CUI – a backbone of national security and on which so much global economic activity and prosperity relies. Whilst this critical infrastructure has traversed the globe for decades, it has until the recent past been largely unreachable and therefore unrecognised as a target of adversary effort. However, vulnerabilities in CUI are now being actively targeted, with our reliance on undersea cables for communications networks and global connectivity presenting an attractive attack surface that we cannot afford to leave unprotected.

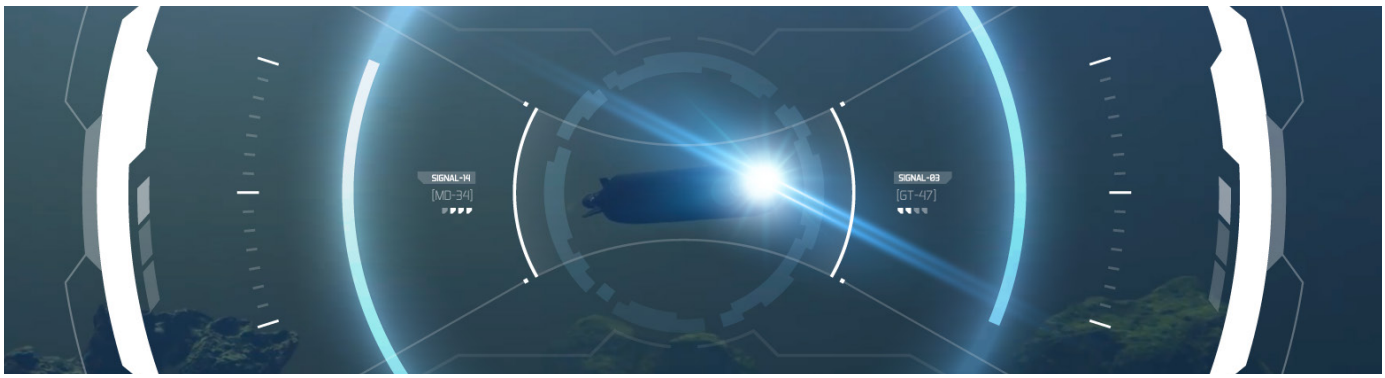
This all points to the scale of the threat to critical undersea cables and subsea defence operations. It is challenging to secure such a large area – particularly in a persistent, cost-effective manner that prioritises sensors, platforms and effectors to proactively detect and deter interference – demonstrating the need for autonomous systems and technologies that can strengthen our ability to prepare for and respond to disruption in the undersea environment. This is what will deliver a much-needed advantage over adversaries.

A missing puzzle piece

Amidst the modern landscape, those responsible for defence and national security are facing an important question: how can we counter today's threats while investing in solutions that will enable us to regain control of the underwater domain?

In short, we need the indicators and warnings to prevent interference or attacks before they happen. This requires sensors and platforms to be ubiquitous, connected (covertly, where necessary) and able to communicate data securely in the theatre of operations in order to accelerate decide and effect functions – fusing intelligence with a common, integrated operating picture available across surface, air, land and space.

However, underwater communications is missing a vital puzzle piece. Our current underwater communications solutions – which still rely primarily on radio frequency technology – are not fit for the digital age. They are low data rate, susceptible to the vagaries of the underwater environment, and vulnerable to variations in water temperature, salinity and refraction – particularly at depth.



This means we are facing a critical capability gap that cannot be allowed to persist. At a time of greater strategic tension between nations, this capability gap is recognised both nationally and internationally – requiring a joint industry and government response focused on exploiting the potential of underwater networked communications and subsea operations.

Indeed, national and international trials and exercise programmes are actively pivoting to focus on uncrewed platforms and the associated networked communications requirements. In the vanguard of these is the REPMUS series of exercises led annually by Portugal in the North Atlantic Portuguese exercise areas. Equally, NATO is setting the demand signal through its Allied Underwater Battlespace Mission Network challenge.

A similar emphasis has also been set by the AUKUS nations as captured in the **2025 Maritime Innovation Challenge**, which focuses on near real time communications between undersea vehicles in a contested and congested environment. What's more, the Royal Navy's CABOT requirement sets the vision of a digitalised North Atlantic underwritten by lean crewed, remotely operated or autonomous uncrewed underwater and surface systems.

> We are facing a critical capability gap that cannot be allowed to persist

Next-generation underwater networking

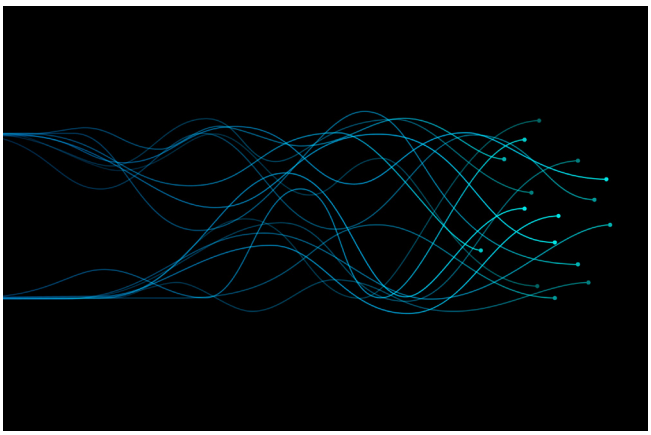
As outlined in the **UK MoD's Maritime Operating Concept** and through **NATO's Digital Ocean initiative**, next-generation underwater networking addresses needs specific to the modern maritime environment. This capability is critical to delivering a network of cooperating platforms, combining both crewed and autonomous vehicles, that together can deliver collaborative and disaggregated capabilities as part of a true system-of-systems approach to maritime operations.

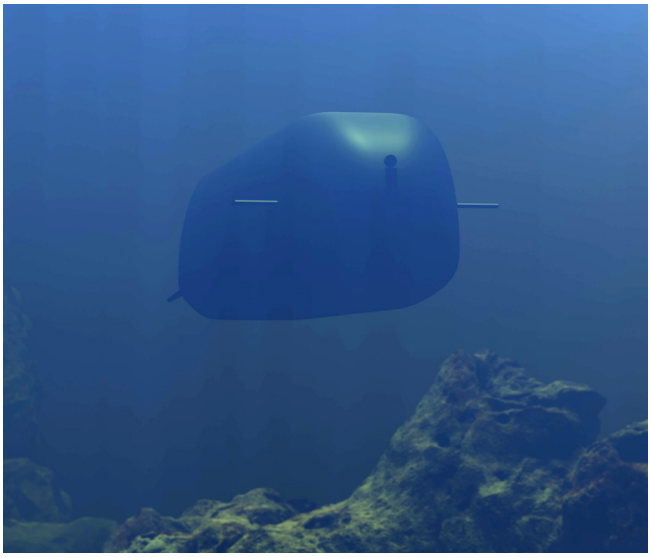
Such a system must be able to provide seamless connectivity between data and communications interfaces. It must support a range of connections including acoustic (through water), optical (through air and water), RF (through air) and cabled. And it must offer a flexible and adaptable solution that can meet the requirements of the network regarding availability, covertness, bandwidth and reach – among other considerations.

Of course, this is no mean feat, as the underwater domain comes with considerable complexity given the harsh nature of the environment. As well as having to deal with a wide range of bandwidth demands, the networking needs of various underwater autonomous systems, seabed infrastructure and crewed platforms will all be slightly different.

But progress within industry is being made. For example, at BAE Systems Digital Intelligence we have demonstrated automatically managed data routing across a multi-node network comprising a mixture of all-through-water, air-water interface, cabled and through-air RF links – testing scenarios that simulate the needs of mine countermeasure and ASW operations.

So, industry is responding to the current threat landscape through the development of underwater platforms and communications technologies that meet today's demands while considering the networking needs of underwater autonomous systems, deployables, seabed infrastructure, surface and crewed platforms, and above water systems. But there is still more to be done on the journey towards building a stable and secure subsea environment.





Payload development and integration

Any underwater communications network needs to support features such as dynamic and mobile network routing, network management, acquisition and authentication, as well as dealing with a wide range of bandwidth demands.

With ongoing developments in agile data networking, the deployment of off-board sensors to conduct data gathering can start to deliver against the need for timely intelligence harvesting. This is particularly relevant when employing sub-surface vehicles.

Challenged with improving the status quo, where data gathered underwater is mostly available for analysis after the mission has completed, the integration of a next-generation underwater networking capability into underwater platforms brings dynamic, mobile network routing into the equation.

To smart, autonomous subsea vehicles capable of edge processing of critical data points, integration of this capability introduces a tangible step towards the provision of in-mission, time sensitive intelligence. Thereby equipping the operator with the necessary indicators and warnings to enable evidence-based decision making.

Taking this a step further, this development will also facilitate the deployment of multiple vehicles simultaneously. This will allow the harvested data to be aggregated and combined to truly provide uncrewed wide-area surveillance at a time when maintenance of the undersea competitive edge is so critical.

Full steam ahead

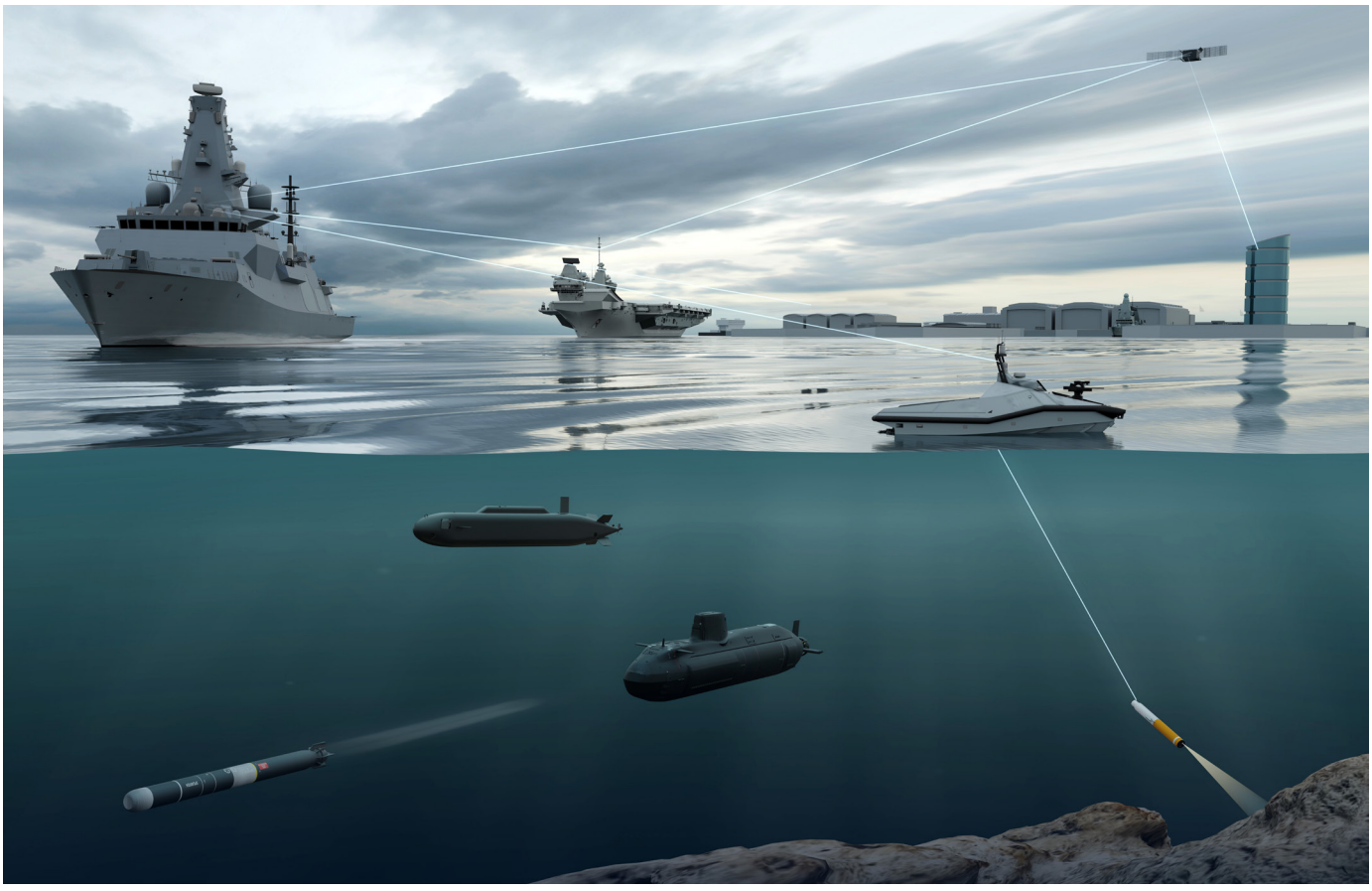
With technological and operational developments bringing geopolitical competition to the underwater battlespace, there is no time to stand still. In the race to build and maintain a **competitive edge in the subsea domain**, where our critical undersea infrastructure is safe and secure from attack or compromise, we must invest in solutions that are equipped to share data and information between sensors, deciders and effectors.

UK industry can take the lead from the **UK Strategic Defence Review**, where the requirement for "…a comprehensive and layered sensor network – operating on, above, and below the water – to create an integrated, multi-domain approach…" is front and centre of capability development for the Royal Navy.

Not only that, as an industry we must continue integrating new capabilities into defence trials and exercise programmes at pace. Testing under exercise conditions can inform and drive future development cycles, while establishing initial operating capability ahead of our adversaries.

Ultimately, the subsea domain is quickly emerging as a new arena of strategic conflict and competition – both from the perspective of prosperity and national security. But, with the right focus, we can engineer the underwater battlespace to our advantage. Integrating capabilities such as next-generation underwater networking represents a tangible step towards the provision of in-mission, time sensitive intelligence – equipping operators with the necessary indicators and warnings to enable evidence-based decision making.

It's innovations such as this which will give the UK and her allies the tools to protect our indispensable undersea infrastructure, achieve secure control of the subsea environment, and look ahead to a future that is stable and prosperous



We are Digital Intelligence

Digital Intelligence is home to over 4,700 digital, cyber and intelligence experts across 16 countries. We operate at the cutting edge of digital innovation and at the heart of organisations that keep vital infrastructure running, national security protected and armed forces prepared. Launched in 2022, Digital Intelligence is part of BAE Systems and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS