

Ocean Robotics Planet

Supported by

BAE SYSTEMS

CRITICAL UNDERSEA INFRASTRUCTURE PROTECTION

CUI

SPECIAL REPORT



3. Flexing muscles:
Norway bulks up civilian-military
co-operation to build CUI security



5. What technologies exist for
Critical Underwater Infrastructure
monitoring and protection?



9. Balancing security and profits with
new strategic realities: Why being
compliant is no longer enough



EDITOR-IN-CHIEF
Richie Enzmann

COPY EDITOR
Will Grant

CONTRIBUTORS
Dr. Lee Willett, John R. Potter, Jan Petter Morten, Steinar Bjørnstad, Cathrine Lagerberg

SALES DIRECTOR
Nick Search

DESIGN & LAYOUT
Milan Farkas

WELCOME TO THE CUI SPECIAL REPORT!

Dear Reader,

This special report focusing on Critical Undersea Infrastructure (CUI) Protection looks at the topic from three different perspectives.

The first article written by Dr Lee Willett is based on an interview with Rear Admiral Oliver Berdal, Chief of the Royal Norwegian Navy, about the cooperation between the private sector and the Navy to tackle the challenge of protecting undersea assets. In Norway, the private sector provides the “muscle”, with the large number of Unmanned Underwater Vehicle (UUV) assets, meanwhile the Navy brings the expertise of surveillance, countering military threats, and mine countermeasures (MCM) to the table. Each party providing what they are good at. This exemplary cooperation should be replicated by other countries and navies of the NATO alliance.

The second article is a comprehensive study written by John Potter, Jan Petter Morten, and Steinar Bjørnstad, a team of academics and experts, that looks at the technical options currently available to monitor and protect CUI. They touch on the current maintenance & monitoring practices, and the key technical resources that are applicable for proactive CUI monitoring. This includes maritime robotic uncrewed

systems, edge computing, AI, distributed acoustic sensing, and satellite systems, just to name a few.

Finally, the report is concluded with an article from Cathrine Lagerberg, who is a technical risk and security expert, about the need for addressing long-term risks when exporting dual-use underwater products or exposing critical information. She makes a valid argument for the need of enhanced export controls when it comes to dual-use technologies. Dual-use technologies could be used by our adversaries against us, because these can be used in weapons and military surveillance, detection, monitoring, planning, construction, and maintenance systems.

I hope you find this thought-provoking report interesting and as a result of it have a better understanding of this challenging and complex issue of CUI monitoring and protection. If you have any questions or comments, please do get in touch.

Best regards,

**Richie Enzmann, Editor-in-Chief,
Ocean Robotics Planet Magazine**

INFO@OCEANROBOTICSPLANET.COM

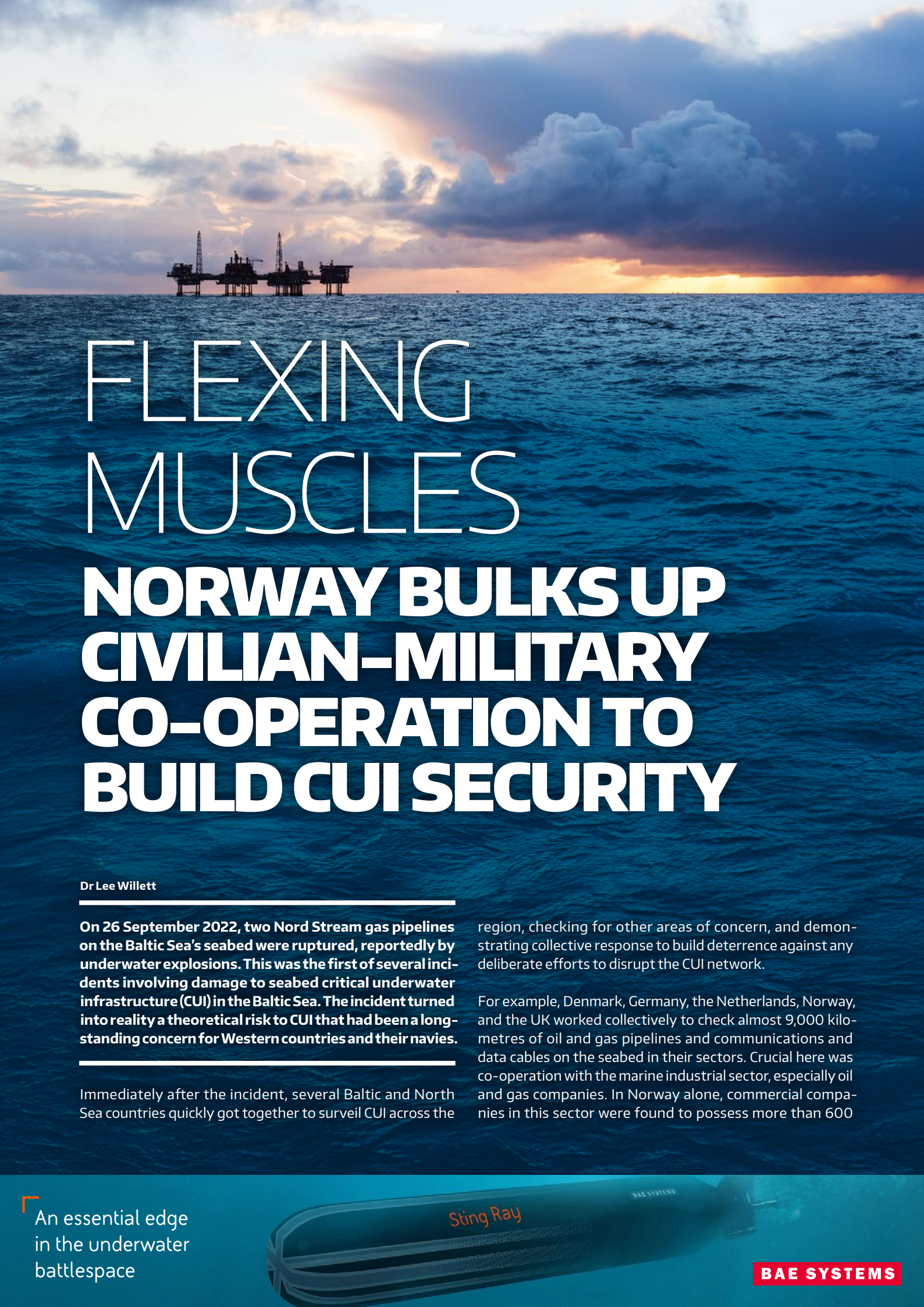


TABLE OF CONTENTS

Page 3. Flexing Muscles: Norway Bulks Up Civilian-Military Co-Operation to Build CUI Security.

Page 5. What available and appropriate technologies exist for Critical Underwater Infrastructure Monitoring and Protection?

Page 9. Balancing Security and Profits with New Realities: Why Being Compliant is No Longer Enough.

A large offshore oil rig is silhouetted against a dramatic sunset sky over the ocean. The sun is low on the horizon, casting a golden glow across the clouds and the water's surface. The rig consists of several interconnected platforms with various structures and cranes.

FLEXING MUSCLES

NORWAY BULKS UP CIVILIAN-MILITARY CO-OPERATION TO BUILD CUI SECURITY

Dr Lee Willett

On 26 September 2022, two Nord Stream gas pipelines on the Baltic Sea's seabed were ruptured, reportedly by underwater explosions. This was the first of several incidents involving damage to seabed critical underwater infrastructure (CUI) in the Baltic Sea. The incident turned into reality a theoretical risk to CUI that had been a long-standing concern for Western countries and their navies.

Immediately after the incident, several Baltic and North Sea countries quickly got together to surveil CUI across the

region, checking for other areas of concern, and demonstrating collective response to build deterrence against any deliberate efforts to disrupt the CUI network.

For example, Denmark, Germany, the Netherlands, Norway, and the UK worked collectively to check almost 9,000 kilometres of oil and gas pipelines and communications and data cables on the seabed in their sectors. Crucial here was co-operation with the marine industrial sector, especially oil and gas companies. In Norway alone, commercial companies in this sector were found to possess more than 600

An essential edge
in the underwater
battlespace



BAE SYSTEMS

uncrewed underwater vehicles (UUVs), providing a deep pool of capability resource that could be drawn from.

The close links between Norway's navy and its seabed-focused commercial sector have been highlighted as a good illustration of effective civilian-military co-operation in securing CUI. Such integrated, collective operations generate what could be termed 'applied mass'. As Royal Norwegian Navy (RNoN) chief Rear Admiral Oliver Berdal explained to Ocean Robotics Planet, the commercial sector brings the "big muscle" of UUV numbers, while the navy can harness this mass with its expertise in surveillance, countering military threats, and integrating different stakeholders to apply the required response.

"First, you have to start with the basic facts: where is the big muscle when it comes to seeing things on the seabed and doing things on the seabed?" asked Rear Adm Berdal. For Norway, the Chief of Navy added, "The big muscle is in the private sector."

Alongside its oil and gas pipeline industry, Norway has significant capacity and expertise on seabed cables, like supplying electrical power and electronic data out to oil rigs and other CUI infrastructure. Alongside sizable shipping and fishing industries, it has growing knowledge in windfarms and other new offshore resource capabilities.

"We have tens of thousands of engineers and people working with seabed problems in private industry every day," said Rear Adm Berdal. "Over the last 50 to 60 years, we've built a huge industry where there's a lot of people with a lot of knowledge, and their everyday job is to do things on the seabed and below the seabed."

"If you need to check 8,800 kilometres of pipelines in the North Sea, do you put grey ships in charge of doing it, or do you use the ships that do this every single day?" the admiral asked, adding that the oil and gas companies regularly and routinely check their pipelines.

Second, the Chief explained, while military forces like navies currently have only handfuls of people with deep expertise in CUI security because the threat is only just starting to surface (despite the long-standing risk concerns), military forces bring deep expertise in two other key areas. For expertise in dealing with explosive devices, "Whether it's historic [ordnance] from the First World War or Second World War, drifting mines, or objects that somebody could place down there, that's where the military expertise and knowledge comes in," said Rear Adm Berdal. Moreover, military forces can combine military intelligence with information from various civilian sources, including national authorities, police forces, coastal administrations, and maritime agencies. The military role here is "getting all the available information and getting it fused to create good situational awareness", the admiral added.

The individual strengths the respective commercial and military stakeholders offer – especially when enhanced today with increased information sharing supported by information

database building – can help accelerate CUI security development, particularly when time is of the essence in deterring or responding to a CUI incident.

"The navy is clearly much better at finding mines than the private sector. The navy is much better at identifying objects and saying 'this is dangerous or not dangerous,'" said Rear Adm Berdal. "However, when you have 8,800 kilometres of seabed pipelines for oil and gas, thousands of kilometres of fibre-optic cables, and thousands of kilometres of electrical interconnectors, if you check all that using the navy's capabilities – even using unmanned, remotely operated vehicles – it will take a long time."

Whether the CUI challenge is responding to an incident in the immediate term or building longer-term deterrence presence, time is of the essence for Western countries, their navies, and the commercial industry they work with. As regards tactical and operational response, and wider strategic impact, "We've covered a lot of ground in a very short time," said Rear Adm Berdal. "When Nord Stream took place, within days an operation was up and running; within weeks and months, a lot of the most important work had been completed," he explained. "Most importantly, during those days, weeks, and months, all relevant actors – on the government side, and on the industry side – were able to get together and discuss things, liaise, and assist each other in a way we'd never done before."

Liaison and other assistance activities are enabled by having staff embedded in each other's operational cells.

"I'm quite sure about one thing," Rear Adm Berdal continued. "If something were to happen again, we would be much quicker the next time – even though we had a pretty fast and impressive reaction the last time – because now we are mentally prepared for it and organizationally prepared for it." The civil-military relationship on CUI security continues to remain close, with meetings frequent and regular, to ensure capacity remains current in response to the threat, he added.

The impact of the threat response was both immediate and long-lasting, the Chief said.

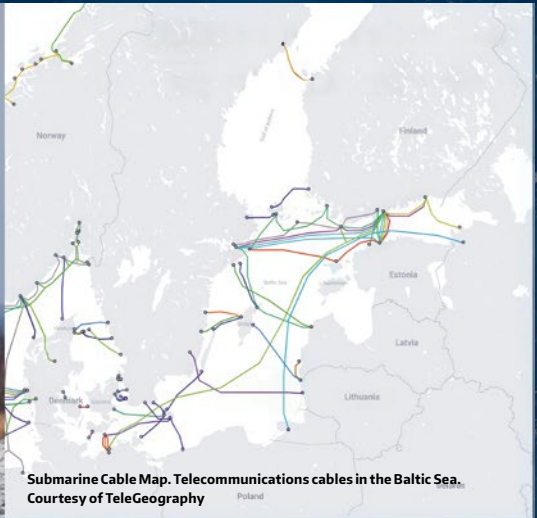
"It was not a 'one-off' thing that we did and then stood down. It was a 'one-off' thing that shook us, that woke us up," he explained. "To a certain extent our responses were tested, and we did quite well – but now we are in a much better situation, much better prepared for whatever may come in the future."

Here, he said, national but also multinational co-operation is key.

"We will still work hard together, especially with allies: I think that's the clue now: one thing is what we do at the national level, but especially now [it's] what we're also doing between countries," the admiral continued. He highlighted bilateral and multilateral co-operation amongst countries responding to several reported and possible CUI cable incidents that have occurred in the Baltic Sea since October 2023.



The vessel New New polar bear photographed missing an anchor after the 2023 Baltic Connector gas pipeline disruption. The anchor was later recovered from seabed. Courtesy of yle.fi



Submarine Cable Map. Telecommunications cables in the Baltic Sea. Courtesy of TeleGeography

WHAT AVAILABLE AND APPROPRIATE TECHNOLOGIES EXIST FOR CRITICAL UNDERWATER INFRASTRUCTURE MONITORING AND PROTECTION?

John R. Potter¹, Jan Petter Morten² and Steinar Bjørnstad³

¹Centre for Geophysical Forecasting, Institute of Electronic Systems, Norges teknisk-naturvitenskapelige universitet (NTNU)

²Alcatel Submarine Networks, Norway

³Tampnet, Norway

In this short commentary we address the issues of who owns, maintains and is currently responsible for Critical Underwater Infrastructure (CUI) with an appraisal of effective technical options that are currently available to monitor and protect them. We conclude that there is a gap in providing coherent protection and that the full power of available solutions is far from realised, largely due to a lack of integration of the disparate parts and the rapid evolution of new technologies yet sparsely appreciated across the stakeholder landscape.

OWNERSHIP, MAINTENANCE, AND THE NEED FOR PROACTIVE MONITORING OF SUBSEA INFRASTRUCTURE

We consider CUI to consist primarily of cables, pipelines and seabed energy production structures. Offshore electrical cables, oil and gas pipelines and seabed production structures are generally owned by large energy corporations with a variety of ownership structures based on specific agreements and regional regulations, which may include national interests and ownerships. Many of these elements

are equipped with Fibre-Optics (FO), embedded in the mixed core of power cables, as a separate cable attached to the exterior of power cables and pipelines or otherwise installed to monitor and communicate with the structures.

Stand-alone subsea FO cables are typically owned by telecommunications companies and consortia formed by these operators. Additionally, major hyperscalers such as Google, Meta, Amazon, and Microsoft invest in and own such infrastructure to support their global data networks.

Operational advantage through integrated training

CURRENT MAINTENANCE AND MONITORING PRACTICES

The responsibility for protection and maintenance of FO cables lies with the owners. Inspections and monitoring of FO cables are generally only conducted when telecom performance degradations occur, meaning damage control is often reactive rather than proactive. Organisations such as the Atlantic Cable Maintenance Agreement (ACMA) and Global Marine perform cable repairs and maintenance when initiated by the owners.

In the case of offshore pipelines, the owners are responsible for routine monitoring and maintenance, carried out according to structured maintenance programs. Specialised subsea inspection companies use Remotely Operated Vehicles (ROVs) and Autonomous Underwater Vehicles (AUVs) to perform periodic inspections, ensuring the integrity of the infrastructure.

Despite their critical importance and relevance to national security, subsea FO cables and oil and gas pipelines are not continuously monitored for or protected against potentially malicious activities in their vicinity. FO cable damage is typically only identified when telecom network performance degrades, while minor oil and gas pipeline damage is usually only discovered during scheduled inspections.

THE NEED FOR PROACTIVE MONITORING

Despite a long history of clandestine cable and pipeline mapping and interference throughout the Cold War, it seems that in the decades of globalisation following the age of détente, little attention was given to the risk of hostile action against the rapidly growing, and often civilian-owned, CUI.

In the light of recent events and geopolitical developments, we now find ourselves motivated to rapidly adapt from focusing on natural hazards to security risk monitoring. This requires a proactive and predictive approach, including deterrence. To achieve this, we need to develop real-time monitoring, with proactive alarm mechanisms.

As shown by recent incidents, trawling and anchor dragging can cause severe damage to submarine cables and pipelines, particularly in areas where cables are insufficiently buried. While some of these incidents are undoubtedly accidental, anchors on some offending vessels have been observed with their tips cut off, so they drag across the seabed rather than dig in as intended by their original design. With only a moderate increase in sophistication, commercially available ROVs can easily be used to deploy explosive charges next to pipelines and other structures.

For oil and gas pipelines, real-time proactive monitoring can both help to prevent damage and reduce inspection costs by enabling targeted inspections when and where an object impact or suspicious activity is detected. Implementing proactive monitoring solutions enhances the resilience of subsea infrastructure, ensuring both operational continuity and cost efficiency.

KEY TECHNICAL RESOURCES APPLICABLE TO CUI PROACTIVE MONITORING

This commentary is too short to be able to list all applicable technologies, so only those that are newly emerging and/or poorly leveraged will be touched upon.

MARITIME UNCREWED ROBOTIC SYSTEMS

As much as we might like, we cannot be in all places at all times, so traditional crewed platforms must be augmented with a fleet of smaller, less expensive uncrewed robotic platforms if we are to achieve the required spatial coverage, temporal resolution and timely intervention that is required. We have seen an explosion of capability in maritime robotics in recent years, maturing from research-level systems to an increasingly complete range of vehicles of all sizes and capabilities for use underwater, on the sea surface and in the air. The range and quality of sensors have also improved dramatically, with smaller, lighter and cheaper sensing systems now available to meet a wide range of requirements. A handful of long-range AUVs could now survey the entire Western European CUI network in a few weeks, compared to the several months that it took to do so following the Nord Stream pipeline incident in 2022. NATO has begun to leverage this potential with TASK FORCE X, but this initiative is still in its early stages and needs to be scaled up to cover a much broader area to be effective for CUI protection across European domains of interest.

EDGE COMPUTING

A significant enabler to maritime robotics is the availability of compact, low cost (in financial, size and weight terms) computational power and memory, combined with advanced miniaturised sensors. These elements in turn allow AI-driven recognition and decision processes to evaluate the environment sensed by the platform to create a local situational awareness in real-time. The crucial benefit of this next-level autonomy is that platforms can now make smart choices about adapting their operational activities in response to their findings, no longer having to wait to pass their data to the outside world and await updated instructions. This dramatically improves the effectiveness and timeliness of robotic platforms.

AI IN THE OUTER SUPERVISORY LAYERS OF A SYSTEM OF SYSTEMS

While AI-driven edge computing is critical to shorten the active control loop for uncrewed systems, AI in the cloud (or, at least, in the outer, supervisory layer of an integrated system of systems) can be used effectively to identify suspicious trends or patterns arising from a disparate number of minor cues that would go unnoticed to human oversight. There are already both military and commercial risk assessment systems being built and offered, based on these ideas. Yet none to date exploit the full range of possible input sensory systems, spanning robotic platforms, shore-based radar, space-based hyperspectral imaging systems, AIS receivers, directional radar antennas, SAR, etc. In addition, AI can infer and predict potentially high-risk scenarios and dubious actors from scouring deep databases of vessels, weather, ports of call, registrations, crew and officers, past incidents, etc. The strength of

synergistic integration lies in the massively increased discriminatory power to reject false alarms, which arise frequently when evaluating the products from only one or a few sensory systems. Data integration enables the detection and flagging of unusual and potentially threatening behaviours in context.

DISTRIBUTED ACOUSTIC SENSING AND STATE OF POLARISATION

Distributed Acoustic Sensing (DAS) uses light backscatter in an optic fibre to measure real-time strain variations along the cable on the metre-scale. In the last few years, DAS has proven capable of detecting earthquakes, explosions, avalanches, meteors, lightning, trawling, anchor dragging, ships, whales, tsunamis, and a great deal more. The list of potential applications is growing rapidly. Specifically, for CUI monitoring, it is possible to detect, identify and track ships and seabed gear, and to separately detect the seabed interface waves caused by the dragging of bottom trawls and anchors across the seabed in the vicinity of FO cables. This can both enable preventive action and remove deniability on the part of the offending vessel.

Most CUI have FO cables as part of the infrastructure, and existing FO cables can be used with a DAS interrogator to monitor activities in the vicinity, with ranges of few km (in the case of bottom dragging) to tens of km (for the detection of surface ships). DAS is not only able to sense propagating acoustic energy but also stresses associated with surface gravity waves. This allows DAS to detect ships not only by their radiated acoustic signature, but also by the pressure signature of their bow and stern waves, which provide an estimate of their speed and length. Any direct interaction with the cable on the seabed can be pinpointed with high accuracy.

Furthermore, measuring the State of Polarisation of laser pulses in a FO cable adds additional information, confirming if a FO cable has indeed been hit or moved. While FO cable owners and operators have been using these technologies for some time, it is still poorly appreciated and only sporadically applied to CUI protection in general.

SATELLITE SYSTEMS

Satellites can be equipped with Automatic Identification System (AIS) receivers, Synthetic Aperture Radar (SAR), Hyperspectral optical imaging and directional radar antennas, all of which are powerful tools to detect and identify surface vessels. Optical imaging is now of sufficient resolution to identify the type of vessel being imaged, if the sky is clear. Hyperspectral imaging helps fill in the gaps, while SAR works in all conditions. Directional radar antennas can be used to locate ships that are using radar, of particular interest if that radar source does not correspond with a valid series of AIS packets.

INFERENCEAL INTEGRATION AND MODELLING

Perhaps the most powerful, yet largely unrealised, technical value is derived by the systemic integration of the many

streams of heterogeneous sensing data to provide a coherent situational awareness. This requires not only the synthesis of many different sensed fields (all with their characteristic ranges, latencies and resolutions) but in the informal inferential Bayesian probability estimation of the probability of a particular vessel, or CUI, being associated with a threat. Several groups, commercial, academic and military, including NATO (e.g. the 'Mainsail' program), are beginning to explore this potential and are finding it to be a rich enabler.

WHAT MIGHT AN INTEGRATED SYSTEM OF SYSTEMS OF THESE TECHNOLOGIES LOOK LIKE?

A suitable integrated system must provide sufficient information to support informed decisions. The data must have both the sensitivity to detect all important interactions and events associated with a developing incident or anomalous behaviour and the discriminatory power to recognise anomalous behaviour in context. This requires high spatial resolution to detect e.g. a cable interaction that is essentially local, on the metre-scale, in addition to a more global appreciation of context. The resolution requirement, together with spatial coverage that could exceed 100 km, enables accurate localisation at considerable distance from the source. This means that we require data with full coverage for very large areas. The combined requirements of high resolution and high coverage drives us to a very high cumulative data rate. For example, FO sensing for a single cable can amount to several TB of data per day. If we are to monitor many cables, with high spatial resolution and at high acoustic bandwidth then we must find a way to deal with massive data flows. It is impractical to continually stream such data rates to a central processing facility, even if it were desirable. The obvious solution is to process automatically at the edge and transmit only important findings.

Edge computing allows us to process data at or near the sensor so that limited digested output can be transmitted and made available to an operations center in near real-time for timely alerts. The output should provide the basis for classification of the type of incident that is developing and, if possible, identify vessels involved. This supports decision making in case an intervention is required.

Fig. 1 illustrates the range of spatial scales of the problem. We need both high resolution and broad coverage, and no single sensing modality can deliver across the vast range of scales, more than eight orders of magnitude. Only a synthesis of many sensing systems can give us the situational awareness we need.

With efficient high coverage sensing we would be able to target the deployment of drones or vessels, including uncrewed, which would be sparsely distributed over the large scales in question. Instead of patrolling the cables or

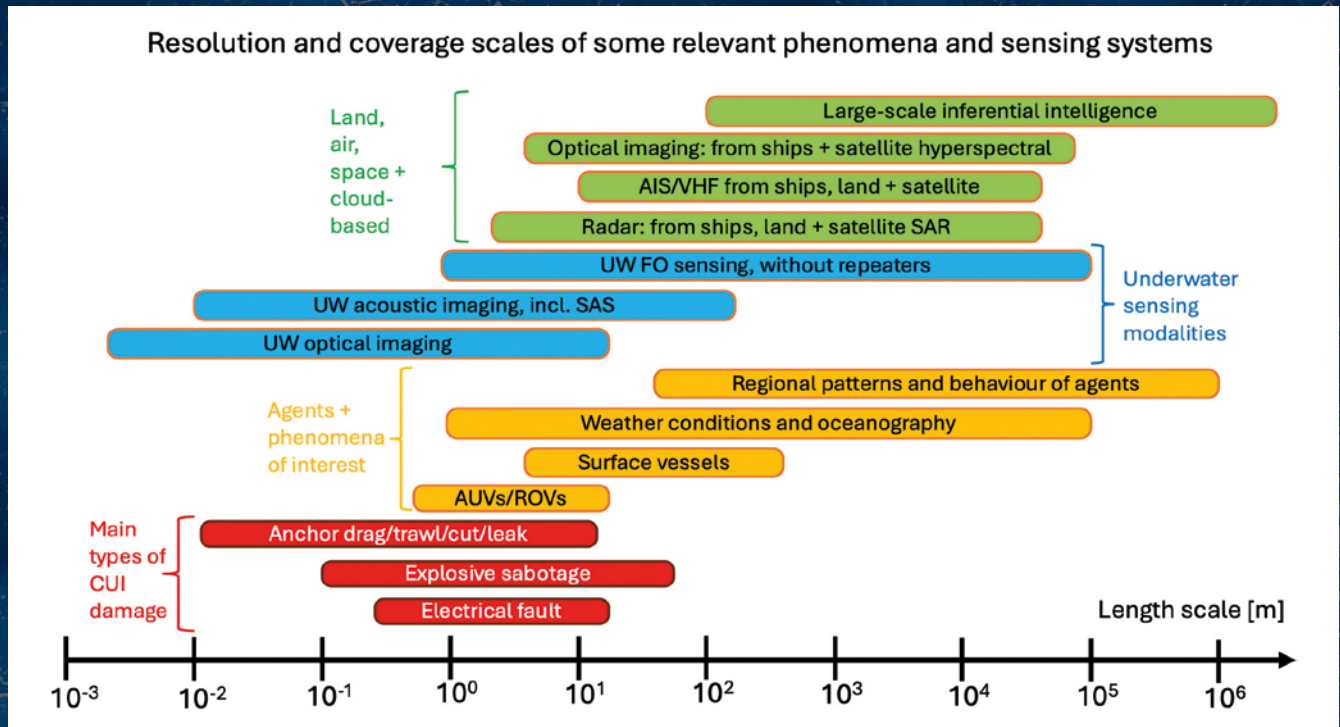


Figure 1. Approximate scales (with granularity/resolution to the left of each bar, and largest relevant scale/coverage to the right) of some features of the problem. The length-scale of interactions causing CUI damage are represented in red. The surface agents and phenomena of relevance necessary to form a good situational awareness are shown in orange. The range of underwater (UW) sensing systems are in blue and above water systems in green. While the scales of interactions and range are only indicative, it is striking that they cover 8 orders of magnitude and obvious that no single sensing system can cover all requirements. FO sensing, using existing cables, greatly adds to our UW capabilities.

pipelines, high spatial coverage data of sufficient resolution enables efficient use of drones or vessels, both crewed and uncrewed, by directing them directly to the location where any anomalous event is developing. Efficient and cost-effective intervention could be implemented by uncrewed surface vessels that can deploy and recover autonomous underwater vehicles and aerial drones.

We consider FO sensing technologies to be a key component, because they provide a data stream that is always on, everywhere on the infrastructure and which does not require any offshore components. When integrated with other sensing modalities, it becomes possible to identify the vessels and mariners involved, who can then be contacted and warned off. Deterrence is the least confrontational and most desirable first-step intervention. Even if the vessel(s) in question continue, denying them deniability is an important component of deterrence and subsequent prosecution of guilty parties.

We also believe that satellite data will be an important component of integrated data interpretation. Satellite optical and radar information have very wide spatial coverage and can be used to track dark vessel activity via several independent sensing modalities, although their temporal resolution may be on the scale of hours and not always useful for real-time situational awareness. Sensors integrated on drones patrolling an area will be characterised by only local coverage but will provide ground truth. These sensors should be of different types that complement the full coverage sensing, e.g. optical (hyperspectral), acoustic, magnetic, EM, to enable appropriate bases for interpretation.

The integrated sensing system envisioned here would provide a very large and dense information pool, with multiple sensing modalities spanning very different spatial and temporal resolutions and coverage and with different latencies. Automated analysis and integration, coupled with AI data mining will be necessary to provide a robust system to raise alerts for important anomalous events and provide support for intervention decisions. A high false alarm rate would reduce operator capacity to follow up on high-risk events and waste resources. Integrating many independent sensing systems with complementary modalities greatly reduces false alarms arising from any individual system. The AI inferential risk profiling we propose will also serve to provide strong guidance for detecting anomalous behaviours in context.

CONCLUSION

Existing technologies could be mobilised to address the current gaps in CUI monitoring and protection, but some of these are relatively new and have not yet been deployed at scale. Examples include FO sensing on existing cables, which provides high resolution monitoring over large spatial scales with real-time data streamed to shore at moderate cost. It is also clear that no single sensing system or platform will suffice, due to limitations on resolution, coverage and false-alarm rate. Multiple sensing systems with different modalities, if appropriately integrated, would be capable of delivering the resolution and coverage required, at much lower false-alarm rates, creating more value than the sum of the parts. AI is a key component, both at the edge (to reduce data volume and provide more intelligent and flexible behaviours) and in the overarching situation assessment, where deep mining for patterns will be necessary to identify anomalous behaviour in context.



BALANCING SECURITY AND PROFITS WITH NEW REALITIES

WHY BEING COMPLIANT IS NO LONGER ENOUGH

by Cathrine Lagerberg, Dual-use, Technical & Strategic Risk and Security Expert, Crown Defense

How can we defend ourselves if we continue selling underwater technology and leaking knowledge to nations we are planning and building defenses against? Most Western companies enforce export control by complying with laws and regulations. However, compliance is no longer enough. The current threat picture demands stricter export controls to remain competitive and safeguard our defense capabilities. Updated decision support, security measures, intelligence-based due diligence and strategic risk assessments: these are all crucial in addressing long-term risks when exporting or exposing critical information to maintain competitiveness and safeguard defense interests.

3dsam79/Shutterstock.com

Cover more underwater
battlespace than ever
before



BAE SYSTEMS

Western technologies are vital for adversaries' military programs and development, hence the establishment of Coordinating Committee for Multilateral Export Controls (CoCom) in 1949 at the beginning of the Cold War. As the Soviet Union once relied upon Western technologies, China is likely facing the same challenges within certain underwater technologies. Until these nations master series-production of similar quality, they will continue to depend on Western components for their military systems. This underscores the necessity for stringent export controls to prevent the transfer of sensitive technologies to countries that the West do not have security cooperation with.

THE ROLE OF MICROELECTRONICS

Modern defense systems, industry, and underwater technologies rely on advanced microelectronics for precise navigation and positioning, reliable communication, target accuracy, and safe and efficient operations. The most advanced microchips are predominantly manufactured in Taiwan on design specifications and orders from U.S. tech companies. Therefore, the U.S. and Western allies currently enforce strict export restrictions to maintain strategic advantage.

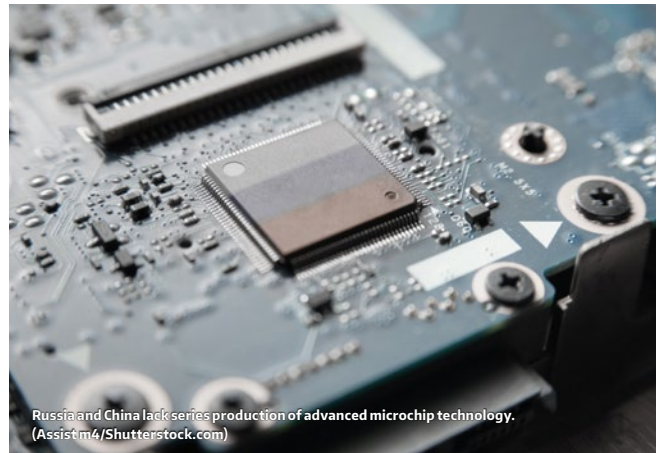
As a result, sanctioned nations must acquire much of this technology through illicit and covert means by circumventing the sanctions. If physical goods cannot be obtained, the next targets will be decision-makers, know-how, R&D, and critical intellectual assets: leveraging collaboration, academia, and industry expertise to gain sensitive access, trade secrets, and strategic information.

Companies developing dual-use (both listed and not-listed) technology must understand that they are part of critical supply chains and make strategic risk assessments accordingly. This includes much more forward-looking and holistic security and risk assessment of employers, research collaborations, supply chains, investors, physical and digital access, in addition to the export itself. All of which can constitute unwanted knowledge transfer to countries that we do not have security cooperation with. Sanctioned entities will pursue vulnerabilities as they arise and target their resources with any tool available to whatever company they're after. Therefore, security must be lifted and holistically assessed and implemented according to today's threat picture, and how we foresee adversaries targeting our technology tomorrow.

STRATEGIC IMPORTANCE OF UNDERWATER TECHNOLOGIES

Underwater technologies are critical for national security and military strategy, from the High North and Arctic – key to NATO and U.S. interests, to the South China Sea and Indian Ocean, where global strategic competition between U.S. and allied forces, including Taiwan, and China is intensifying.

Nations like Russia and China are developing advanced underwater capabilities. Strategic nuclear assets and autonomous systems rely on high-quality Western microelectronics



Russia and China lack series production of advanced microchip technology. (Assistm4/Shutterstock.com)

and sensors for mapping, collection, intelligence gathering, and autonomous operations. Some of these technologies are under the limit of ITAR and Wassenaar specifications, or contain items that are not considered "very critical".

It's impossible to create an exhaustive list of microelectronics and inertial navigation systems (INS). However, without the best of them, your underwater assets will drift off, you can miss your targets, end up with inaccurate maps or positions, lose communication between mothership, modem, transponders and platforms being operated, or conduct unsafe and hazardous operations.

Given the strategic importance of underwater technologies, current export control measures are inadequate if we want to prevent adversaries from acquiring critical technologies.

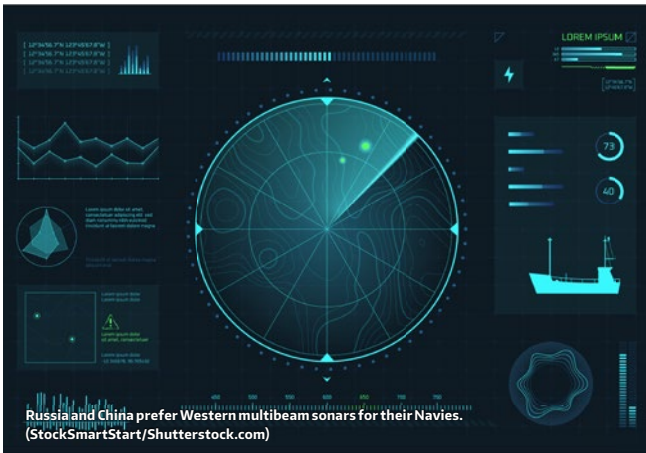
THE NEED FOR ENHANCED EXPORT CONTROLS

Unauthorised transfers of Western technologies and knowledge could enhance adversaries' military capabilities and pose significant security and strategic risks. And there is really no such thing as a civilian end user. All civilian vessels and equipment are likely to be placed at state or military disposal if needed. According to the Norwegian Intelligence Service's annual report Focus 2025:

"The use of civilian technology in military weapons programmes challenges traditional export controls. Civilian technology can be used in weapons and military surveillance, detection, monitoring, planning, construction, and maintenance systems. Russia, China, Iran, and North Korea [...] use a variety of methods to obtain and exploit civilian Western technology for military purposes".

Hence, the likelihood of exporting to a civilian end-user that ends up being used military will always be high.

Many businesses in Europe struggle to navigate China. The export of "listed" dual-use goods for military use to China is not permitted, however, it is highly challenging to ensure export for civilian purpose since China's national law, Article 7, obligates Chinese individuals and organisations to support national intelligence work.



It's therefore imperative to:

- | Include a broader range of dual-use technologies, encompassing also commercial items and non-listed/non-ITAR items;
- | Take the Chinese national law into account: the risk of diversion to intelligence and military purposes can never be less than 50%;
- | Extend risk assessments to include comprehensive strategic and intelligence-based due diligence and screening, to identify potential threats associated with technology transfers, and assess the risk of diversion to military end-use. These assessments must include employees, sub-vendors, third party contractors, R&D, and any exposure that critical defence suppliers and tech companies have towards entities and companies we do not have security cooperation with.

WALK THE WALK NOT TALK THE TALK

Complying with laws and regulations is not enough, as regulations are often the result of reactive and long bureaucratic processes and regime consensus.

International frameworks established to define and regulate export of dual-use goods and technologies, like the Wassenaar Arrangement and Missile Technology Control Regime (MTCR), face inherent limitations due to the diverse and sometimes conflicting interests of their member countries with opposing defense strategies and national priorities.

As Chris Lade (Saab UK)'s emphasises in his article "Fortifying Undersea Security", there is an urgency in joining forces between commercial and defence sector since most of the technology for safeguarding critical undersea infrastructure (CUI) is delivered by the private and commercial industry. Since the same technology can be used against CUI; to detect, map and collect information for intelligence purposes and future offensive military missions, these companies have become our last line of defence.

Companies must therefore embrace their responsibility by enforcing stricter export control and security routines. Turning

a blind eye and continuing business as usual will not only weaken our defense and military strategies, but also lead to loss of market, lost competitiveness, and adversaries gaining crucial technology: ultimately risking the West's technological lead.

By adopting more strategic security, risk, and export assessments, companies will not only gain a competitive advantage against your competitors, but they will also be in a stronger position to increase market position, and expand market share while mitigating long-term risks. But this will require more than just compliance.

SECURING CRITICAL TECH AND KNOWLEDGE IS EVERYONE'S RESPONSIBILITY

No department or service will do it for you. They may warn you, fine you, or, in the worst case, put you in jail if you fail to comply. But ultimately, the responsibility lies with the company itself, which is perhaps the core of the problem: disclaimer of responsibility.

The authorities must establish requirements and regulations that follow the threat landscape, so it becomes easier for businesses – and not up to the company – to decide when and how to secure the values that will ultimately affect national and international security interests.

Loopholes exist to be circumvented. We cannot rely on disclaimers and written end-use, re-export, prohibited use, or third-party restrictions clauses. These are easy to bypass, and adversaries don't care.

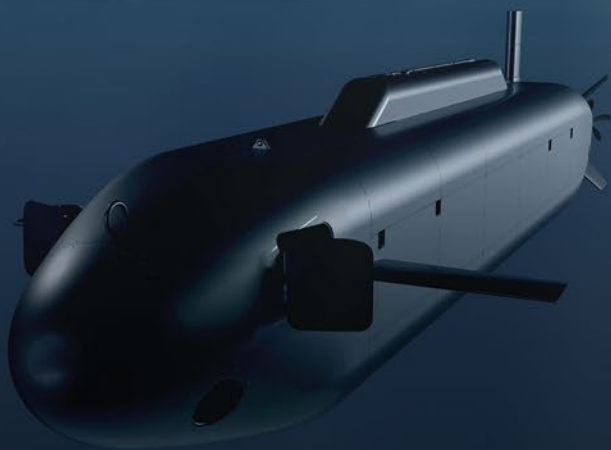
Next time you wonder whether to export or not, maybe the answer is in the question itself. It's better to consult an expert one too many times and do some extra due diligence, than finding your sonar on an adversary's research ship mapping your nation's/allies' infrastructure.

There's a lot to think about, but if each of us takes slightly more responsibility for our exports, it accumulates and makes a real impact. One thing is for certain: compliance alone is no longer enough.

Data driven support



BAE SYSTEMS



Ocean Robotics Planet

Supported by

BAE SYSTEMS



**CRITICAL UNDERSEA
INFRASTRUCTURE PROTECTION**

SPECIAL REPORT