EYES IN THE SKIES

Maël Torca explores pioneering advanced solutions for underwater security challenges

The underwater environment, integral to global maritime operations, is increasingly recognised as critical to international security. This domain encompasses not only the vast underwater expanses, but also the vital infrastructure located beneath the ocean's surface. These include subsea communication cables, pipelines and other critical assets essential to global connectivity and energy supply. Traditionally, this area has not been the focus of terrorist activities, but emerging threats and technological advancements are changing this landscape. Unseenlabs, a French company founded in 2015, is at the forefront of protecting these underwater environments through its space-based radio frequency detection technology. With a constellation of 15 satellites in orbit, Unseenlabs can detect RF signals emitted by ships worldwide, in any weather conditions, offering capabilities to monitor and secure the underwater domain.

The underwater environment presents unique security challenges, particularly concerning the protection of critical infrastructure such as subsea communication cables and energy pipelines. These infrastructures are crucial for global communications and the transportation of energy resources, forming the backbone of international connectivity and economic stability. However, their remote and often isolated locations make them difficult to monitor and protect, exposing them to significant risks.

One of the most pressing threats is the potential for sabotage. An attack on these infrastructures could lead to cascading failures across multiple sectors, including finance, communications and energy. For example, the severing of a single subsea cable could isolate entire regions from the global internet, disrupting essential services such as banking, air traffic control and emergency response systems. The ripple effects of such an incident can create widespread economic and geopolitical instability.

Another serious concern is the threat posed by unauthorised vessels that may attempt to operate covertly near these infrastructures. By deactivating their Automatic Identification System (AIS) transponders, these vessels can become 'invisible', allowing them to approach and potentially damage critical underwater assets without detection. Such actions, whether intentional or accidental, can result in severe consequences, including major communication outages, interruptions in energy supplies and environmental disasters like oil spills or gas leaks. Such incidents not only disrupt global operations, but also have long-term ecological and economic repercussions.

Historically, the underwater environment has not been a primary target for terrorist activities due to several key factors. One of the main reasons is the technical complexity involved in conducting operations below the ocean's surface. Sabotage or other illegal activities underwater require advanced expertise, specialised equipment, and significant financial resources, which many terrorist groups lack. The need for submarines, remotely operated vehicles or specialised diving equipment, along with the technical knowledge to use them, creates a high barrier to entry.

Maritime terrorism poses unique challenges due to the vastness of the ocean and the logistical complexities involved in executing such operations. Unlike land-based attacks that can utilise local knowledge and infrastructure, maritime operations demand extensive planning, significant resources and coordination over large distances. Positioning a vessel for an attack, maintaining secrecy and avoiding detection are far more complex at sea than on land.

Additionally, the United Nations Convention on the Law of the Sea (UNCLOS) emphasises freedom of navigation, which complicates efforts to regulate and monitor vessels that might pose a threat. This legal framework, while essential for maintaining order and facilitating global trade, can inadvertently provide cover for malicious actors. UNCLOS allows ships to pass through territorial waters and exclusive economic zones with minimal interference, which terrorists can exploit to carry out operations under the guise of legitimate maritime activities.

Furthermore, terrorist groups often prefer targets that guarantee high visibility and immediate impact. Land-based and surface vessel attacks offer the media exposure and psychological impact these groups seek to spread fear and gain attention. In contrast, the underwater domain, while critically important, does not provide the same level of immediate visibility, making it a less attractive target. The lack of media coverage and public awareness reduces the perceived value of underwater targets for those looking to maximise psychological impact.

UNCLOS does not specifically address maritime terrorism, making it difficult to counteract such activities

within its legal framework. While international efforts, such as the International Ship and Port Facility Security Code and the Suppression of Unlawful Acts Convention, aim to enhance security, these measures must be balanced with the rights granted under UNCLOS. This balance can lead to conflicts between necessary security measures and legal rights, underscoring the need for a more integrated approach to maritime security that addresses both legal and operational challenges in combating terrorism at sea.

THE EVOLVING NATURE OF THREATS NECESSITATES A PROACTIVE APPROACH TO UNDERWATER SECURITY

Despite the historical challenges associated with targeting the underwater environment, several factors suggest that this domain could become more attractive to terrorist groups and other malicious actors in the future. Technological advancements are making it easier and more cost-effective to operate undetected below the ocean's surface. The development of smaller, more affordable unmanned underwater vehicles and other submersible technologies is lowering the barriers to entry for underwater operations. These advancements mean that terrorist groups or rogue actors could potentially acquire the capability to conduct underwater operations without the need for large-scale, sophisticated infrastructure.

In addition, the growing strategic value of underwater infrastructure, such as subsea cables and pipelines, is elevating these assets as potential targets. Terrorist groups may view attacks on these infrastructures as a means to cause widespread disruption, attract international attention and exert pressure on governments and corporations. The ability to disrupt global communications or energy supplies could have a significant psychological and economic impact, making these infrastructures attractive targets despite the operational challenges involved.

Geopolitical tensions, particularly in contested maritime regions, can also incentivise non-state actors to exploit vulnerabilities in underwater environments. For example, regions rich in energy resources or those hosting critical communication infrastructure are becoming increasingly important to global security, making the protection of these underwater assets a priority. In regions like the South China Sea, the Arctic, or the Eastern Mediterranean, where territorial disputes and competition for resources are intensifying, the risk of underwater sabotage or terrorism is heightened.

The potential for environmental and economic warfare is another factor driving the increased focus on underwater security. Terrorist groups or rogue actors may recognise the potential for underwater attacks to cause significant environmental damage, such as oil spills or gas leaks, leading to long-term economic and political instability. The ability to create an environmental disaster, such as a large-scale oil spill, can have devastating consequences for local economies, ecosystems, and public health, while also serving as a powerful tool for spreading fear and exerting political pressure. These factors combined suggest a shifting dynamic where the

With the ability to detect RF signals globally, satellite technology is essential for identifying any potential threats

underwater domain is becoming a more attractive and feasible target for malicious activities.

Unseenlabs provides solutions to address the emerging threats to underwater security through its space-based RF detection technology. With its constellation of 15 satellites in orbit, Unseenlabs can detect and monitor RF signals emitted by vessels across the globe, even those attempting to operate covertly by turning off their AIS transponders. This capability is crucial for identifying potential threats in real-time, allowing for swift and decisive action to protect underwater infrastructure.

MARITIME TERRORISM POSES UNIQUE CHALLENGES DUE TO THE VASTNESS OF THE OCEAN

The unique technology is particularly effective in monitoring the proximity of vessels to critical underwater assets, such as subsea cables and pipelines. By detecting anomalies in RF emissions, Unseenlabs can identify unauthorised or suspicious vessels that may pose a threat to these infrastructures. This capability enables stakeholders, including governments, defence agencies and commercial operators, to take proactive measures to safeguard their assets before any damage can occur.

This technology is also invaluable in regions where geopolitical tensions are high and the risk of maritime incidents is elevated. By providing continuous monitoring of the maritime domain, The technology can help prevent incidents before they escalate into full-blown crises. This proactive approach to maritime security is essential in today's interconnected world, where the stakes are higher than ever.

The underwater environment, with its critical infrastructures like subsea communication cables and energy pipelines, is increasingly becoming a focal point for global security concerns. Traditionally overlooked by terrorist groups due to the technical challenges and logistical complexities involved, this domain is now more vulnerable due to advancements in technology and growing geopolitical tensions. As the strategic value of these underwater assets rises, so does the risk of them becoming targets for sabotage or other malicious activities.
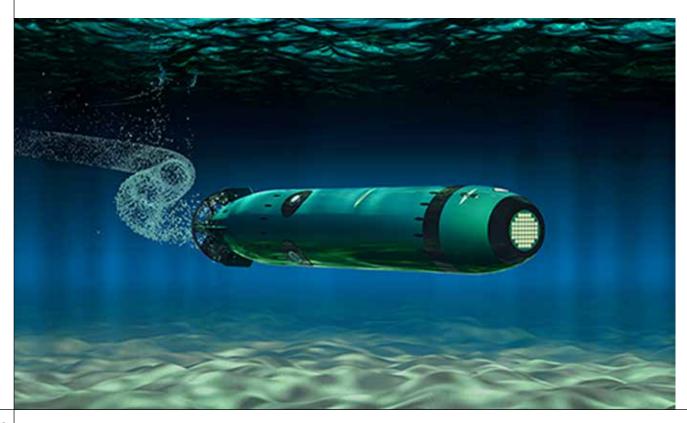
The evolving nature of these threats necessitates a robust and proactive approach to underwater security. The ability to detect and monitor potential threats in real-time, especially from vessels attempting to operate covertly, is crucial for protecting these vital infrastructures. As the world continues to rely heavily on underwater networks for communication and energy transport, the need for continuous monitoring and advanced threat detection becomes more critical.

Organisations like Unseenlabs play a vital role in this effort by providing the technological means to monitor the maritime domain effectively. With the ability to detect RF signals globally, including from vessels that may attempt to evade detection, such technology is essential in identifying and mitigating potential threats before they escalate. By leveraging these capabilities, stakeholders can enhance the protection of underwater infrastructures, ensuring the stability and security of global operations.

Addressing these challenges requires a combination of technological innovation, international cooperation and a comprehensive understanding of the legal frameworks governing maritime activities. By integrating these elements, stakeholders can better safeguard the underwater domain, ensuring the continued security and stability of global operations that depend on these essential infrastructures. As threats continue to evolve, so too must the strategies and technologies used to protect the underwater environment, making it imperative for all involved to stay ahead of potential risks and to act decisively in the face of new challenges ●

Maël Torca joined Unseenlabs in February 2022 as a Communications Officer, specialising in writing and English translation. He studied literature in preparatory literary classes and holds a bachelor's degree in English studies. He then pursued a master's degree in communication before joining Unseenlabs.

Terrorist groups could potentially acquire the capability to conduct underwater operations without the need for large-scale, sophisticated infrastructure