NEW SPACE-BASED RADIO FREQUENCY DETECTION TECHNOLOGY APPLIED TO MARITIME SURVEILLANCE FOR SUBSEA CABLE NETWORKS

Clément Galic, Damien Pigasse, Olivier Michel, Jean-Charles Gondet, Rachid Nedjar, Lucile Castella, Hélène Dupriez (Unseenlabs) & Hervé Février (Landelles Consulting)

Email: clement.galic@unseenlabs.fr
Unseenlabs / 15 rue Claude Chappe – 35510 Cesson-Sevigné – France

Abstract: This paper explores the growing importance of maritime surveillance amid increasing global maritime traffic and subsea cable construction. AIS (Automatic Identification System), initially introduced to improve safety, has limitations such as signal congestion, spoofing, and coverage gaps. Detection of radio frequencies (RF) emitted by vessels offers a complementary solution, ensuring broader coverage and identifying even "dark vessels." An RF data collection campaign (Oct–Dec 2024) in the Celtic Sea revealed critical insights, including undetected "dark vessels." The study shows how RF data strengthens subsea cable security—supporting installation, monitoring, and incident response, and boosting the overall efficiency of subsea projects.

1. WHY IS MARITIME SURVEILLANCE BECOMING INCREASINGLY ESSENTIAL?

The maritime sector has seen a dramatic increase in both traffic and construction of subsea cables in recent decades. These changes have brought a series of new challenges that require more sophisticated surveillance methods. With an estimated 80% of international trade in goods being transported by sea [1], and the rapid growth of subsea cable networks, the importance of maritime traffic surveillance to protect critical infrastructure cannot be overstated.

1.1. Growth in Maritime Traffic and Cable Construction

The surge in maritime traffic is directly correlated with the expansion of subsea cable networks. As global connectivity has increased, the demand for high-capacity data transfer across continents has spurred the construction of new subsea cables. Between 2019 and 2021 alone, international bandwidth usage doubled reaching nearly 2,900 Tbps [2]. The expansion of submarine cables is primarily driven by the soaring demand for data transmission—especially from hyperscalers such as cloud providers and online platforms—whose infrastructure needs have scaled dramatically. Additionally, this expansion is also driven by operators and countries aiming to build redundancy into submarine cable networks – minimizing the risk of service disruptions and strengthening overall network resilience. As a result, between 2014 and 2024, approximately 687,000 kilometers of submarine cables were deployed worldwide, averaging about 67,700 kilometers per year [3]. This trend is illustrated in Figure 1.

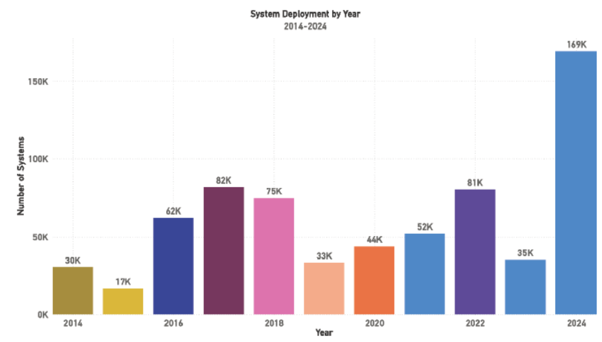

Figure 1
Source: *SUBMARINE TELECOMS INDUSTRY REPORT 2024 | 2025 [3]*

As of early 2025, according to Telegeography [4], approximately 1.5 million kilometers of subsea cables are currently in operation, with nearly one million additional kilometers planned over the next decade. These cables underpin almost all global internet connectivity, communications, and financial services. Given their critical importance, safeguarding subsea cables is essential and requires effective surveillance of maritime traffic that could potentially threaten this vital infrastructure.

1.2. Subsea Cable Damage – Context and Challenges

Despite advances in subsea cable technology and deployment methods—including improved routing and

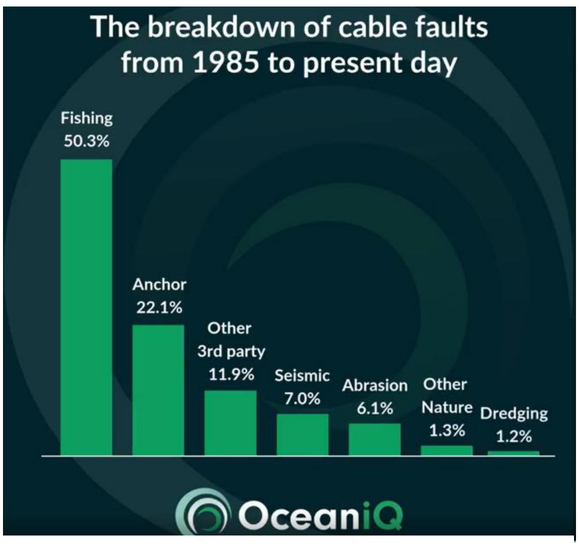

Figure 2
Source: *OceanIQ [Linkedin post] on March 13, 2025*

sophisticated laying operations—these cables remain susceptible to physical damage, particularly in shallow waters less than 400 meters deep. According to the ICPC (2022) [5], the primary causes of cable disruptions include fishing activities, ship anchoring, and natural disasters. Supporting this, recent data published by OceanIQ on cable faults from 1985 to the present indicates that over 72% of faults result from anchoring or fishing activities (see Figure 2). Implementing enhanced maritime surveillance in these vulnerable zones could help mitigate, or even preempt, such disruptions.

Meanwhile, geopolitical tensions have underscored the importance of heightened surveillance measures for subsea cables, recognized as strategic assets essential for global communications and economic stability. In response, multiple international organizations and initiatives have emerged to bolster protective efforts. For instance, the European Union has developed strategic plans to safeguard subsea cable infrastructure, acknowledging the increased risks of sabotage or disruption. Similarly, the International Advisory Body for Submarine Cable Resilience, in collaboration with the International Telecommunication Union (ITU), was established to address emerging risks and promote stakeholder cooperation. NATO's Baltic Sentry mission represents another critical effort, specifically designed to secure undersea cables within the Baltic Sea region. These efforts reflect a global commitment to enhancing the security and resilience of vital subsea infrastructure amid growing geopolitical uncertainties.

Furthermore, there has been a rise in the number of vessels suspected of conducting espionage or mapping activities near submarine cables, exemplified by Russia’s spy ship Yantar.

Since Russia's invasion of Ukraine in 2022, Russian military and government-linked ships have been spotted in UK waters more than 40 times, with nine incidents near subsea data cables and energy infrastructure as reported by *The Times* [6].

2. WHY IS CURRENT MARITIME SURVEILLANCE TECHNOLOGY NOT ENOUGH?

Although maritime surveillance technologies like AIS (Automatic Identification System), VMS (Vessel Monitoring Systems), and coastal radar have advanced, they still fall short of providing full and reliable coverage of global maritime traffic.

These systems, while useful in enhancing safety and regulatory compliance in some regions, still have some limitations that prevent them from offering a full and accurate picture of maritime activities.

2.1. The Limits of Cooperative Tracking Systems

A major limitation is that cooperative tracking systems are not universally required. For example, while AIS is widely used by larger vessels, it is not mandatory for many smaller ones. In some areas, especially within the global fishing fleet, only 2% of vessels use AIS according to Global Fishing Watch [7], creating major visibility gaps in maritime monitoring. Without extensive adoption, a significant portion of maritime traffic is left unmonitored, creating substantial gaps in our ability to accurately assess traffic, especially in more remote or international waters.

The declarative nature of these systems also introduces a vulnerability: they operate on the principle of cooperation, meaning vessels can opt to disable or manipulate their tracking signals—whether intentionally or due to technical failures. This leaves the system open to deliberate falsification, such as ghost positions, where ships falsely appear to be in different locations, or the complete absence of tracking data when systems are turned off.

Such manipulations undermine the integrity of maritime data, making it difficult for authorities to get a true sense of what is happening at sea, especially in regions where enforcement is weaker or absent like in international waters. A study conducted by Iphar et al. [8], using an EBIOS risk analysis, highlights potential threats and scenarios arising from the transmission of incorrect AIS data. There are four specific types of AIS spoofing used to evade sanctions, as illustrated in Figure 3.

Figure 3: 4 types of AIS spoofing
Source: Starboard [9]

To fill these gaps, surface and subsea drones, along with Maritime Autonomous Surface Ships (MASS), could be in the future used to protect subsea cables in targeted areas. These technologies offer high-resolution imagery and can operate surveys or inspect cable infrastructure directly. However, their effectiveness is often limited by factors such as range, environmental conditions, and the need for constant deployment. By contrast, RF data enables wide-area, persistent monitoring, capable of identifying vessels in areas where drones or MASS may not be viable.

2.2. The Challenges in Monitoring Remote Waters and Illegal Activities

Even when ships are tracked using radar systems, these technologies are limited by their range and the quality of data they provide. Coastal radar stations can only detect ships within line of sight, leaving vast areas of open ocean—particularly in the high seas—virtually unmonitored. This results in significant blind spots where maritime traffic, including illegal activities such as unreported fishing, unauthorized migration, or smuggling, can go unnoticed. The inability to effectively monitor these remote and expansive areas further exacerbates the challenges of maritime security and hampers the enforcement of international laws and regulations.

These coverage gaps are especially concerning as global shipping expands and maritime operations grow increasingly complex. Without an effective, reliable way to track all vessels—regardless of size or location—current systems fall short in delivering the situational awareness needed for safety, environmental protection, and legal enforcement at sea.

This is where radio frequency (RF) data comes into play—unlocking a new era of maritime surveillance. RF data has the potential to revolutionize maritime monitoring by providing accurate, continuous, and far-reaching coverage, bridging the gaps left by conventional systems.

2.3. Space-Based RF Detection for an Enhanced Maritime Domain Awareness

Over the past decade, the global space industry has undergone major transformation driven by the rise of nanosatellites. This technological revolution has made it possible to launch small, cost-effective, and highly capable satellites into orbit**.** Unlike traditional large satellites, which are expensive and complex to build and deploy, nanosatellites—typically weighing between 1 and 10 kilograms—offer a faster, more affordable alternative. They support a vast range of applications, from Earth observation to communications and data collection, with the added benefits of shorter development cycles and greater operational flexibility.

While nanosatellites have reshaped access to space, enabling more cost-effective and versatile satellite solutions, another groundbreaking technology is emerging in the field of radio frequency (RF) detection: mono-satellite technology. This approach uses single satellites to monitor RF signals in real time, offering highly specialized capabilities that enhance and extend the benefits of nanosatellite systems. At the forefront of this advancement is Unseenlabs, the only company in the world leveraging dedicated mono-satellites for RF signal detection.

Unseenlabs delivers unique data by detecting radio frequency (RF) signals emitted by ships across vast areas at sea (see Figure 4 for an example of navigation radar detection).

Their RF signature is geolocated and characterized, allowing for the monitoring of uncooperative ships, also known as "dark

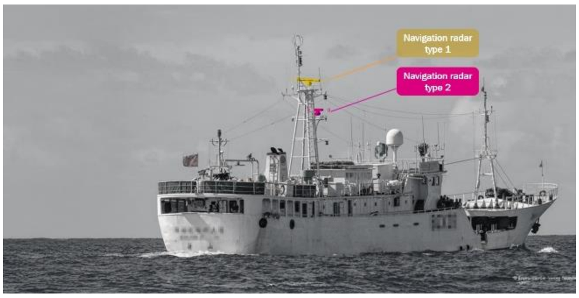

Figure 4 : Navigation radar illustration
Source: @Unseenlabs

ships or vessels", regardless of their distance from the coast and independently of their conventional maritime security systems (AIS, VMS, or LRIT - Long-Range Identification and Tracking).

With a steadily growing fleet of 16 mono-satellites, Unseenlabs operates its constellation commercially on a daily basis. Each satellite pass covers a wide footprint—approximately 300,000 km² (see Figure 5 for a visualization of typical coverage per collection).

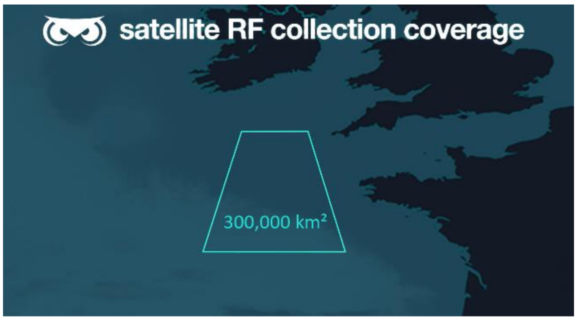

Figure 5: Radio frequency data collection coverage
Source: @Unseenlabs

The service offers also a high revisit rate over each monitored area— up to 12 times a day — and a latency of 2 to 6 hours from data collection to final delivery.
Then, the data produced can be combined with other available data sources such as SAR (Synthetic Aperture Radar), optical imagery, VMS, for deeper or more targeted analysis.

Maritime security actors (coast guards, navies, customs, or private entities) gain a more comprehensive view of actual maritime traffic with improved ability to focus on specific areas of interest. This approach also helps optimize the deployment of naval and aerial resources, that are often limited and costly, for more effective on-site monitoring of concealed activities at sea.

3. UNVEILING THE INVISIBLE: RF INTELLIGENCE USE CASE FOR SUBSEA CABLES IN THE CELTIC SEA

3.1. Context in the Celtic Sea

The Celtic Sea, located between the southern coasts of Ireland, Great Britain, and the western shores of Brittany (France), is a unique marine region within the Atlantic Ocean. Its bathymetry is primarily characterized by a continental shelf with a depth ranging from 60 m to 600 m, gradually descending into deeper abyssal plains.

In our use case, the focus is on seabeds shallower than 400 m, as these areas are more prone to snags and anchor-related incidents — particularly from fishing activities.

The region's varied underwater topography plays a significant role in shaping local marine ecosystems and, in turn, the fishing practices used. The Celtic Sea is known for its demersal fish populations, which are primarily targeted through bottom trawling methods, especially the "pêche arrière" technique. This involves towing a funnel-shaped net along the seabed to effectively capture demersal and benthic species.

Beyond its ecological and economic importance, the Celtic Sea is also a critical route for global telecommunications. Numerous submarine cables traverse the region, facilitating intercontinental data exchange. Among these, the Celtic Interconnector stands out as a major ongoing project. This 575-kilometer submarine electricity cable will connect La Martyre in Brittany, France, to Cork, Ireland.

3.2. Unveiling Hidden Activity in the Celtic Sea: RF Data Collection Above Subsea Cables

A radio frequency (RF) detection campaign was conducted in the Celtic Sea during October, November, and December 2024, resulting in a total of 61 data collections.
Each campaign covers more than 300,000 km² (see Figure 5 for an illustration of coverage area). During this campaign, Unseenlabs' satellite constellation detected 4,842 emitters. The key value of this RF data collection is its ability to detect all vessels, including those not visible through legacy monitoring systems. It is important to note that this number does not directly indicate the number of vessels in the area. First, the number of emitters is cumulative across all collections. Second, a single vessel may carry multiple transmitters.

3.2.1. Analysis of Fishing Vessels and Undeclared Positions

For example, data from December shows that 19.90% of detected positions were not visible through the AIS monitoring system (see Figure 6).

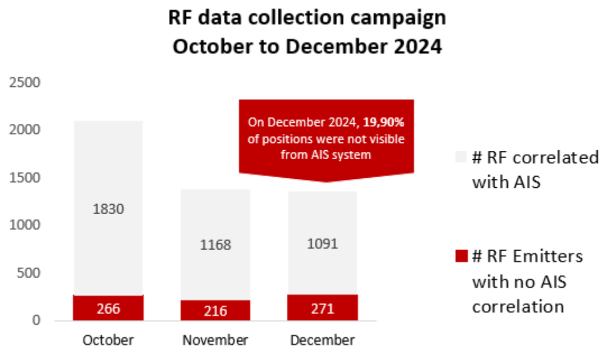

Figure 6: Analysis of RF data campaign from Oct-Dec 2024
Source: @Unseenlabs

One particularly interesting area in this analysis lies at the intersection of the exclusive economic zones (EEZs) of Ireland and the United Kingdom, near the 400-meter bathymetric boundary. In December, AIS-correlated emitters in this zone (see Figure 7) were predominantly fishing vessels. The numbers shown in the hexagonal cells represent the count of unique vessels reporting fishing activity. All of these vessels, each over 23 meters in length, were located above the 400-meter depth threshold.

Figure 7: RF positions correlated with AIS - Number of fishing vessel
Source: @Unseenlabs

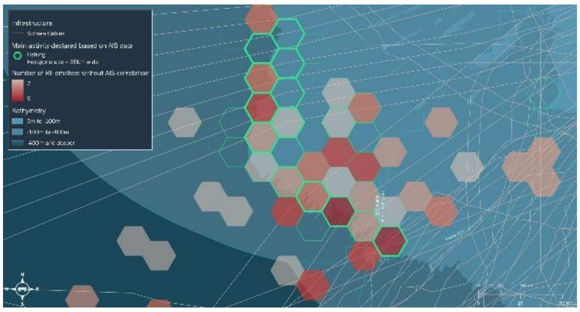

Figure 8: RF emitters with no AIS correlation (RF-only) circled by fishing types
Source: @Unseenlabs

The Figure 8 overlays this fishing vessel typology with RF only detections—emitters that could not be matched with AIS data.
These RF only positions represent potential "dark vessels" that could be involved in Illegal, Unreported, and Unregulated (IUU) activities. However, it is also possible that some of these vessels operate legally, using a Vessel Monitoring System (VMS) without broadcasting AIS signals, and are therefore compliant but invisible to traditional AIS-based monitoring. Notably, the highest concentration of these undeclared positions occurs in areas dominated by fishing vessels and lies above zones where multiple submarine cables are present.

3.2.2. The Added-Value of RF Data for the Subsea Cable Industry

The correlation between undeclared activity and high fishing vessel density underscores the importance of continuous monitoring and analysis. Figure 9 provides a comprehensive and detailed view of the campaign's coverage, highlighting all detected emitters

Figure 9: Unseenlabs final product sample
Source: @Unseenlabs

and distinguishing between those correlated with AIS and those not.

This map adds valuable context to the analysis. This case study in the Celtic Sea is one of many RF data campaigns conducted in regions of strategic interest to the subsea cable industry, including the Baltic Sea, the South China Sea, and others.

For the subsea cable industry, RF data is an essential tool across every phase of a project, offering valuable insights that support installation planning, ongoing operations, and long-term maintenance. Before the cable is laid, access to historical data on undeclared maritime activities in the proposed area is essential. RF data provides a comprehensive overview of the region's maritime traffic — including dark vessels, allowing companies to assess the feasibility of the location and anticipate potential risks to the project.

Once infrastructure is deployed, RF data supports ongoing monitoring of geofenced areas around subsea cables and platforms. This near real-time data provides exhaustive security insights, enabling operators to detect illegal activities or risks posed by unreported vessels. By anticipating potential incidents, operators can adopt proactive risk management strategies to reduce disruptions and maintain operational safety.

In the event of an incident, whether accidental or intentional, RF data can assist investigations by providing valuable historical insights—if the area had been previously monitored. When data is available, it enables more precise forensic analysis, helps identify vessels potentially involved (if emitters were detected at least once), and sheds light on activity patterns at the time of the event.
This data can significantly enhance insurance claims handling, compliance checks, and legal proceedings, ensuring more effective and timely responses.

To conclude, space-based RF detection greatly improves the ability to plan future cable routes or platform installations based on live and historical data, to monitor illegal activities or risks near subsea infrastructure, and to investigate past incidents for compliance, forensic analysis, and damage assessment. By integrating RF data into the full lifecycle of subsea cable projects, companies can enhance security, optimize installation processes, and ensure ongoing operational security.

4. REFERENCES

[1] UNCTAD, "With an estimated of over 80% of the volume of international trade in goods being transported by sea," UNCTAD report, available at: https://unctad.org/meeting/launch-review-maritime-transport-2024 (Accessed on March 31, 2025).

[2] TeleGeography, "The State of the Network 2023 edition – Demand Trends," publication, p.3, available at: https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2023.pdf (Accessed on March 31, 2025).

[3] SubTel Forum, "Submarine Telecoms Industry Report 2024 | 2025," publication, p.69, available at: https://subtelforum.com/industry-report/ (Accessed on March 31, 2025).

[4] TeleGeography, "As of early 2025, we believe there are over 1.48 million kilometers of submarine cables in service globally," Submarine Cable FAQs, available at: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions (Accessed on March 31, 2025).

[5] ICPC, "Submarine cables and the oceans: connecting the world," publication, available at:

https://www.iscpc.org/publications/ (Accessed on March 31, 2025).

[6] The Times, "Russian ships in UK waters amid Ukraine conflict," news article, January 23, 2025, available at: https://www.thetimes.com/uk/defence/article/russian-ships-uk-waters-ukraine-3k8962h72?region=global (Accessed on March 31, 2025).

[7] Global Fishing Watch, "Only 2% of vessels use AIS," available at: https://globalfishingwatch.org/our-technology/ (Accessed on March 31, 2025).

[8] Iphar C., Napoli A., Ray C., Alincourt E., Brosset D., "Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety," ESREL 2016, Glasgow, United Kingdom, pp.606–613, ISBN 978-1-138-02997-2.

[9] Pole Star, "AIS Spoofing," Starboard article, available at: https://www.polestarglobal.com/resources/ais-spoofing/(Accessed on March 31, 2025).