INSS Special Publication

The Challenge of Defending Underwater Communication Infrastructures

Yuval Eylon | June 29, 2023

Underwater infrastructures are a rapidly evolving domain – worldwide, as well as in Israel. This developing phenomenon stems from the need to define and address the emergence of potential threats and disruptions endangering worldwide communication infrastructure. Such infrastructure can be differentiated by the depth of its deployment, and thus the investment in force buildup differs accordingly. Shallow water defense, up to 50 meters, draws most of the attention, while deeper deployed assets should be dealt with by intelligence and alert, prevention, and deterrence, damage containment, reconstruction, if necessary, and redundancy. At the same time, intelligence and technological efforts are required to cope with the accelerated development of autonomous unmanned underwater vehicles in recent years. The world of underwater infrastructures in general, and underwater communication infrastructures in particular, is fertile ground for international cooperation, since these infrastructures are submerged in national and international territorial waters. The challenges evolving from the need to protect and maintain such infrastructures, along with the complexity and costs involved in developing the relevant capabilities, are shared by many states, especially those near the Mediterranean.

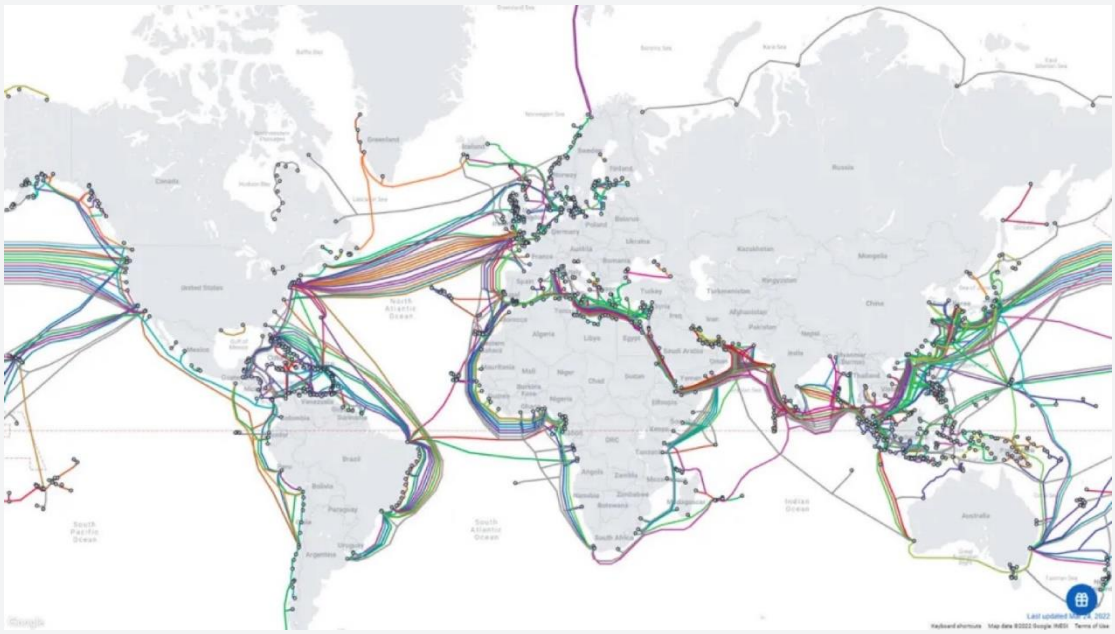
Underwater Communication Infrastructure

The vast majority of global communication is supported and provided by underwater cables. More than 95 percent of global communications (voice and data) pass through these cables, while the remaining 5 percent are satellite-based. More than 500,000 miles of underwater communication cables are positioned on the ocean floor providing communication for globalization networking. These cables are primarily fiber optic, with data rate roughly equal to 150 million simultaneous phone calls. Israel is connected to the world through a single-digit number of underwater cables, providing the main communication channel with the world for all civil and defense-related information.

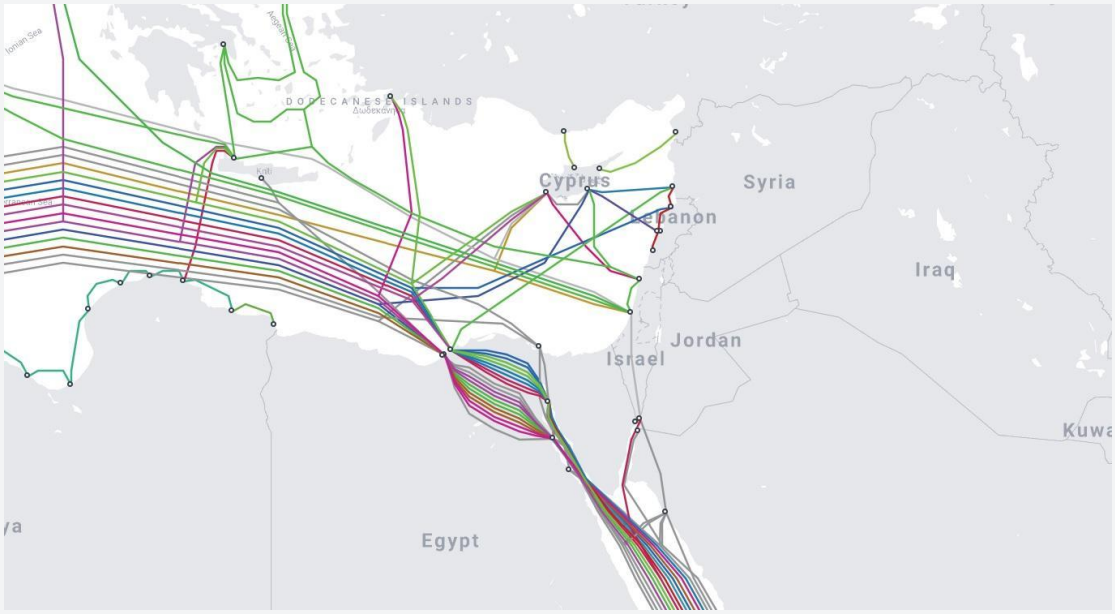
As mentioned, worldwide voice and data communication is underwater fiber optic-based. This technology has become the technology of choice, while the only alternative is satellite-based communication. There are thousands of miles of underwater fiber-optic cables, enhanced by line-amplifiers located along these cables. The chosen option is advantageous: it has a much higher transfer rate, and the distances that data have to “travel” are significantly shorter, which enables higher transfer speed with minimal latency. Furthermore, the transfer of information using underwater cables is considerably more secure, requiring less encryption and encoding (not allowing eavesdropping), compared to transmission of information via satellite transmission. As a result, underwater fiber optic cables provide all internet communications,

international trade, and communication between various governmental and private entities worldwide. The legal counsel of the International Cable Protection Committee (ICPC) estimates that the cost of damage to an international underwater communication cable is $1.5 million per hour.

Submarine communication cables are deployed by special purpose ships, with a high degree of professionalism, skill, and complex technical capabilities, including detailed mapping capabilities, utilizing unmanned vehicles operating in significant depths. All over the world, there are around 40 ships performing this task, all of which are owned by private companies providing their services to communication corporations or governmental customers. Some 200 underwater cables are damaged annually. Seventy-five percent of the damage is caused inadvertently by fishing equipment and ship anchors. Apparently, the remaining 25 percent of the damage is deliberate.



Worldwide fiber-optic cable distribution | Source: Techspot



Eastern Mediterranean cable distribution | Source: TeleGeography

As shown, so far the global voice and data communication is based on a worldwide web of fiber optic cables, located at the seabed of oceans and seas. This unique communication infrastructure is a strategic and tactical tool of all nations and countries, stemming from recent state of the art technological advancements. These worldwide infrastructures must be handled as a unique asset, due to the distinct environment in which they operate, the singular technologies they use, and skills required to deploy and maintain it. At the same time, threats to this unique worldwide essential capability must be examined and analyzed, accordingly.

Handling aspects of the threat has gained momentum worldwide, and proactive thinking and attention is emerging from various entities, such as specific countries, international organizations, and commercial companies. Consequently, international terror, whether state originated or terror organization-initiated, must be examined. Moreover, political changes underway, around the world in general and in the Middle East in particular, have altered the nature of the various threatening elements. Therefore, the means used to protect existing and future infrastructures must be sharp and cutting-edge.

Damage Analysis

Deliberate attacks against underwater communication cables are not a new phenomenon, and numerous such incidents occurred in the past. During the World Wars, the British cut the German underwater communication cable, and over the years, other navies and countries caused similar damage. However, damage to underwater communication assets by terrorist organizations or pirates is a rather new phenomenon that has gained momentum in recent years. For example, in 2007 Vietnamese pirates attacked a cable deploying ship; in another incident, optic cable amplifiers were stolen, resulting in the suspension of communication for 79 days. Another act of terror near the coast of Egypt in 2013 included cutting cables and loss of communication. Also, several attempts by various countries, mainly superpowers,

to hook up to the communication cables in order to “bug” information transferred through them have been noticed.

Recent state-of the art developments of underwater capabilities, such as long-range midget unmanned submersible vehicles and remotely controlled submarine robots, contribute to underwater infrastructures deployment and maintenance, and constitute a threat when deployed for sabotage, manipulation, or harm to underwater infrastructure. Such action could critically damage international as well as domestic communication assets and expose its user to a variety of threats, such as disclosure or loss of information transmitted through the mentioned infrastructure.

Standard defense techniques such as mobile marine infrastructures (boats), as well as stationary infrastructures (rigs and buoys), are studied and addressed, yet the issue of underwater communication infrastructure is still in its early stages, particularly in Israel. The rapid pace at which relevant threats develop creates the need to define and address advanced and appropriate defense tactics and assets as soon as possible.

Israel, as an “island,” due to its unique geo-strategic position, prevents it from developing ground links and compels it to rely almost completely on underwater infrastructure to maintain its communication links with the world. At the same time, there is increasing potential for damage or malign connection to communication cables in the Mediterranean. Actors in the Mediterranean arena, such as with the establishment of the Russian presence, Turkey’s ambition to gain influence in the maritime arena, Iran’s ongoing efforts to enhance its influence in the area, and numerous terrorist organizations all together pose a considerable threat to Israel’s communication, as well to its potential allies.

Defending Underwater Transmission Infrastructures

Everyone that wishes to protect its maritime assets, whether above water or underwater, has, above all, to deploy “sea control” – in other words, monitor the maritime arena, above and under water, regularly and continuously over an indefinite period of time, to detect and recognize all actors and their assets operating within that area. As a result, one can identify and track suspicious or hostile activities within his arena. To execute such control, it is necessary to acquire and deploy capabilities similar to those used to control the national airspace by air forces, only tailored to fit the maritime environment and requirements.

The vast geographic dimensions of national maritime arenas along with the underwater volume in international water where the communication assets are positioned in addition to the complex environment require that the sea control approach be formulated carefully. Area and depth specificity are of major importance, as are the volume of submarine infrastructure contained and the potential threats in the area.

Threats to Underwater Infrastructure

Threats in the underwater domain should not be analyzed primarily based on depth layers, and not in the traditional way, based on threat types and origin. Secondary analysis should differentiate threat types, namely terrorist organizations, states,

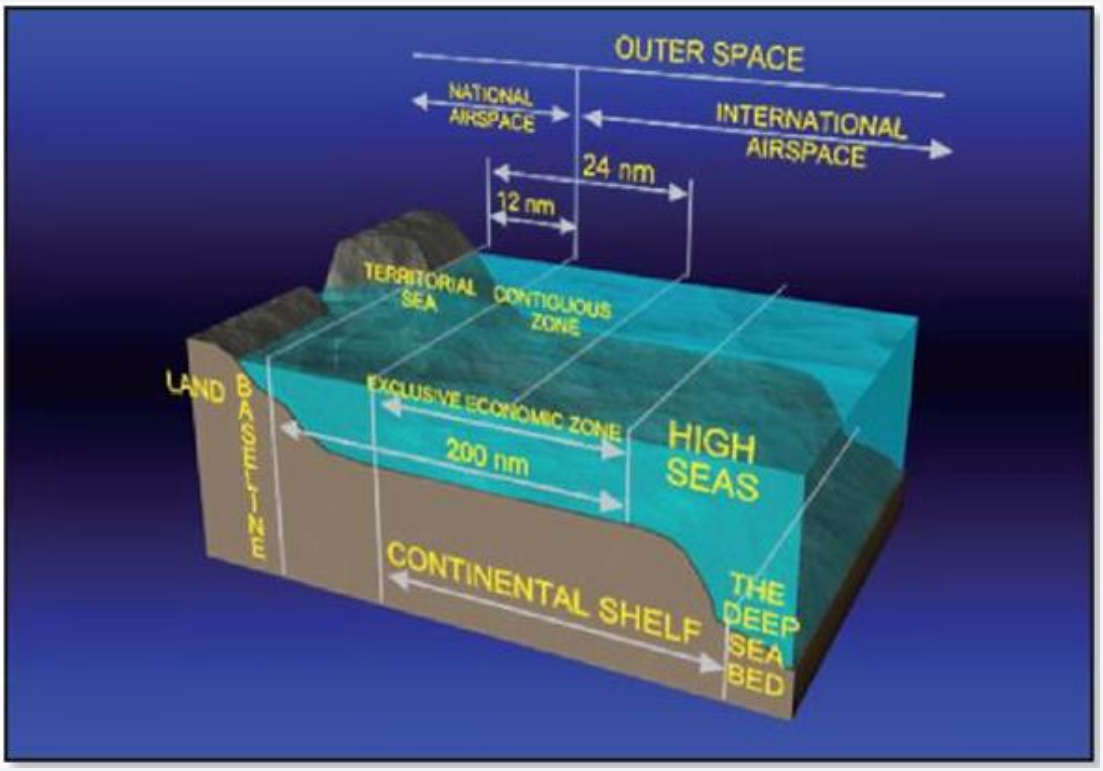
superpowers, and more. Moreover, threat types and origins are changing. For example, today states use various organizations as proxies to carry out missions against strategic capabilities of other states, in an attempt to avoid being identified as the aggressor.

Following is a categorization table, demonstrating the thesis:

Threat	**Depth**	**Type of conflict**	**Effect**
Unmanned underwater vehicle	0-5,000 meters	• Limited conflict: Terrorist organizations / semi-state organizations • War: States + limited conflict players	All communication assets
Divers	0-50 meters	• Limited conflict: Terrorist organizations / semi-state organizations • War: States + limited conflict players	Communication assets close to shore
Submarine	Approx. 0-500 meters	• All type of conflicts	All communication assets
Midget submarine	Approx. 0-200 meters	• Limited conflict: semi-state organizations /states • War: States + limited conflict players	All communication assets

Based on the above table, it is obvious that “volume defense” could be the optimal defense of the communication infrastructure. Unfortunately, it is most complex, due to its enormous dimensions, and has technical and logistic limitations when applied to the vast volume that must be covered, if and when used for communication infrastructure defense.

Although modern technology enables the creation of underwater imaging (through sonar and other means), it is relatively short-range, compared to above water and aerial images. Therefore, when it comes to defending underwater infrastructures, one must consider alternative solutions.



Sea depth layer visualization | Source: 2b1st Consulting

Depth Layer Protection and Defense

This paper suggests a depth layer defense approach, to handle current threats to underwater infrastructure. The proposed concept assumes application of known naval operational concepts tailored to cope with underwater threats in accordance with the depth at which the infrastructure is located. Operational concepts suggested are: intelligence and alert, deterrence and prevention, spatial defense (overwater defense and underwater volume protection), close defense, and damage containment/reconstruction and redundancy. Each operational concept will be applied and operated in the depth layer at which its impact is optimal for the defense against underwater communication threat.

Intelligence and alert: The maritime arena itself poses many challenges to intelligence, due to the high number of participating actors, both at the strategic and the tactical level. Fortunately, underwater threats, particularly advanced threats, require high skill and advance deployment, which leaves a signature and can be tracked in time by existing alert means.

Intelligence and alert operations can be divided into two:

a. Tracking capabilities and intentions in time: The size of the area in which response to underwater threats is required and their complexity require early warning capabilities. Creation of relevant intelligence picture is possible if all the relevant sources are integrated, with shared responsibility. International cooperation based on shared interests is highly important. Since the threat to underwater communication infrastructures is a simultaneous threat to countries

sharing infrastructure located within the exclusive economic zone or territorial waters of several countries, the integration of assets and alert operation are joint interests and can be enhanced by international agreements and resource allocation.

b. Potential real-time response and threat minimization require real-time data collection and analysis capabilities. Controlling underwater territory in open seas is highly complex. Alternatively, control must be limited to underwater infrastructure relevant areas. The picture of the relevant underwater domain can be achieved by means of mobile as well as stationary systems (buoys, extended arrays). Extended arrays are effective in a relatively long range, varying from hundreds of meters to several kilometers. These systems can provide the means for alert with an emphasis on intelligence gathering prior to an attack.

Furthermore, controlling a territory entails the creation of a combined overwater and underwater image. While underwater data will be collected, as stated above, the surface data will be gathered complementary means. The surface arena includes many targets – civilian vessels, merchant fleets, unidentified vessels, foreign military vessels, fishing boats, and enemy ships. The use of advanced means of detection – satellites, ground, naval, or airborne radars, visible intelligence systems – can provide data and alert for all vessels present within a given territory. Inter-organizational and interstate utilization of advanced identification technologies combined with intelligence information enables the tracking of vessels engaged in suspicious activities and providing threat alerts for under and surface water traffic.

Prevention and deterrence: Prevention can be initiated, even before the arrival of the threatening element at the scene. This capability is especially important when dealing with autonomous underwater vehicles, since the possibility of detecting and tracking them is currently rather limited. Deterrence would be achieved by preemptive attacks before they are carried out or through presence at the scene, over as well as under water.

Spatial defense: Spatial defense of underwater transmission infrastructures areas requires many resources, since continuous awareness is required. This type of defense is relevant mainly for territorial waters, and to some degree for exclusive economic zones as well. It would include vessels equipped with means to cover above and underwater control with means for launching underwater control and volume protection within the underwater arena.

Close protection of the infrastructure itself: Such protection would impair the effectiveness of the attack and the ability to strike the target or navigate in its vicinity. It would be attained through passive protection or striking the actual threat. Such protection, in various configurations, is relevant to all areas and all depths, using tools tailored to the type of threats and to specific locations. Close protection can be applied to the entire infrastructure or locally, at locations or points designated as the “center of gravity” of the infrastructure.

Damage containment and redundancy: In order to maintain underwater communication to the maximum, repair reconstruction capabilities must be included in case of damage, while maintaining operational continuity as much as possible.

Investment in every aspect of force buildup and the method for deploying defense systems depends on the depth at which the infrastructure is located. Generally speaking, most attention should currently be given to areas of shallow water – 50 meters or less. At other depths, emphasis should be put mainly on intelligence and alert, prevention and deterrence, damage containment, reconstruction, if needed, and redundancy. At the same time, intelligence and technological efforts are required to cope with the accelerated development of autonomous unmanned submarine vehicles seen in recent years. The world of underwater infrastructures in general, and underwater communication infrastructures in particular, creates fertile ground for international cooperation, since they lie on the seabed, within the sovereign territory of various states as well as international waters. The challenges presented by the need to defend and maintain infrastructures, along with the complexity and costs involved in developing capabilities for coping with such challenges, are shared by many maritime nations, especially along the coasts of the Mediterranean.