From the Strait of Hormuz to the Ocean Floors: When War Stops Being Visible and Becomes Systemic

Published on 25/04/2026

In recent days, media linked to Iran have published a detailed map of the submarine cables crossing the Persian Gulf, the Red Sea, and the Strait of Hormuz, bringing attention to one of the least visible but most critical elements of global infrastructure, namely that physical network that enables the very functioning of the internet and connects continents, economies, and financial systems through underwater corridors where enormous volumes of data transit daily, making everything we consider normal today possible, from communications to economic transactions, to the cloud services on which an increasing part of our society relies.

A Physical, Locatable, and Strategic Infrastructure

The publication of this map does not introduce anything new from a technical standpoint, but it has the merit of making evident something that has remained outside the public debate for years, namely the fact that this infrastructure exists, is physical, is locatable, and, above all,

develops in geographical areas that are not neutral but characterized by tensions, strategic interests, and operational capabilities that cannot be ignored. For this reason, the value of this publication is not so much informative as communicative, because placed in the current context, it assumes the meaning of a message addressed to a very specific interlocutor.

From Hormuz to the Digital Domain

The context is that of an increasingly evident clash between Iran and the United States, centered precisely on the control of the Strait of Hormuz, which has always been one of the main global energy choke points and which in recent months has returned to the center of a dynamic of mutual pressure made of blockades, threats, and shows of force, with concrete effects on commercial traffic and global economic balances. It is precisely within this tug-of-war that the publication of an apparently technical map assumes a different meaning, because it does not merely describe an infrastructure, but implicitly suggests an extension of the field of confrontation, shifting attention from what has always been considered the heart of the problem — oil — to something less visible but potentially just as impactful, namely digital connectivity.

The New Invisible Targets

In all conflicts, we are used to thinking of evident, known, and often in-the-open targets, such as military bases, energy infrastructures, bridges, logistical nodes, and everything that falls within the classic perception of war and defense, namely what is visible, mappable, and defensible through traditional systems, men, means, and technology. However, the evolution of our society has progressively shifted the focus towards completely different targets, less conspicuous but no less critical, effectively creating a new category of vulnerability that escapes common perception but represents one of the true sensitive points of the system.

The Arteries of the Digital World

Today, there exists an infrastructure that is not protected by perimeters, not guarded by soldiers armed to the teeth, not covered by radar or advanced defense systems, and precisely for this reason tends to remain outside the collective imagination, but in reality constitutes the base on which everything else rests. It is represented by hundreds of fiber optic cables laid on the seabed, often no thicker than a garden hose, that cross the oceans connecting different continents and carrying almost all global data traffic, effectively becoming the true arteries of the digital world.

A Vulnerability Difficult, but Not Impossible to Exploit

These infrastructures, precisely because of their nature, are difficult to reach for an improvised actor, but they are not at all impossible to locate or hit for those with adequate technical and operational capabilities, and above all, they are not impossible to disrupt. Every year, in fact, numerous incidents are recorded, often caused by seemingly trivial activities such as fishing or ship anchoring, demonstrating how thin the margin is between the normal functioning of the system and its interruption.

The Problem of Digital Choke Points

The point, however, is not vulnerability in an absolute sense, because any infrastructure is, but the fact that this vulnerability is concentrated and systemic. The global network is not distributed uniformly, but tends to converge in certain mandatory geographical corridors, real choke points, where multiple lines overlap creating a structural dependency that, under normal conditions, represents an advantage in terms of efficiency, but in crisis conditions can quickly become a risk factor.

Redundancy Is Not Infinite

Naturally, there are redundancy mechanisms, and data traffic can be diverted to alternative routes in case of a single line interruption, but this capacity is not infinite. Above all, it only really works when the alternatives are independent of each other, while it loses effectiveness when multiple cables share the same geographical corridors, because in that case the problem is not eliminated but simply distributed, with effects that translate into slowdowns, congestion, and, in the most severe cases, real regional service interruptions.

Why Satellites Are Not Enough

At this point, it is essential to clarify an often misunderstood aspect, namely the idea that there are alternative systems capable of truly replacing submarine cables in case of interruption. While it is true that in public debate satellites are often thought of as a possible parallel network, the technical reality is much clearer: these systems represent only a marginal component of global connectivity and not a true alternative to the physical backbone, being limited in terms of capacity, latency, and operational sustainability, while almost all intercontinental traffic continues to travel through submarine cables.

A Network That Relies on Itself

This means that there is no true redundancy on completely different systems, but rather a network that relies on itself, multiplying the paths but maintaining the same basic principle: traffic passes through physical cables, and when these fail, what remains is not a fully functioning alternative system, but a residual capacity entirely insufficient to support the normal functioning of economies, financial markets, and digital services on a large scale.

The Difference with Energy

Unlike what happens in the energy sector, where there are alternative modes of transport — as in the case of gas that can be moved by ship compensating at least partially for the interruption of a pipeline — in the case of global connectivity this flexibility simply does not exist. The internet, in its intercontinental dimension, cannot be transferred to a different infrastructure without suffering significant degradation, and it is precisely this absence of a real alternative that transforms a technical vulnerability into a strategic dependency.

The Strategic Leverage of Connectivity

And it is precisely here that the Iranian message assumes its deepest meaning. Just as the Strait of Hormuz has historically been used as a lever of pressure on the energy level, the publication of this map suggests that even the digital dimension can be transformed into a strategic lever, not necessarily through a direct attack, but simply by making evident where the pressure points are, like in a poker game where showing the cards is not meant to play them immediately, but to change the opponent's behavior.

The Nord Stream Precedent

In this context, the parallel with Nord Stream becomes immediate not so much for a direct similarity between the two infrastructures, but for the principle it represents: hitting a critical physical infrastructure, often invisible to the general public, means intervening directly on the functioning of society, creating effects that go far beyond the immediate damage and that propagate throughout the entire system.

The Gray Zone of Degradation

The real point, therefore, is not to imagine extreme scenarios in which “the internet shuts down,” but to understand that there is a much more realistic and, in some ways, more

dangerous gray zone, in which the infrastructure continues to function but in a degraded manner, creating systemic effects that are difficult to attribute, manage, and counter.

Vulnerability as an Operational Advantage

The real question, at this point, is not whether these infrastructures are vulnerable, because they are by definition, but how much we are willing to accept this vulnerability as part of the system, until someone decides to turn it into an operational advantage.