3 Main Points

1. How vulnerable are undersea cables, and what are the implications of their sabotage for security and global stability? 2.Undersea cables, carrying 95% of global data, are critical to communication, defense, and finance but are increasingly targeted. Attacks expose risks like physical damage and tapping, threatening economic and energy stability. 3.With 1.4 million km of cables worldwide, urgent action is needed to protect this critical infrastructure from growing threats.

About the Author

Mihnea Turcitu is pursuing a B.Sc. in International Relations and Organizations at Leiden University (NL). His research focuses on the Middle East region. Currently, he is a board member of a foundation dedicated to helping refugees integrate into the academic world in the Netherlands.

Working in Darkness

Brief by Mihnea Turcitu

Brief:

Undersea cables, the shadow workers of our economy, defense and communication.

As some might have noticed these cables have recently come into the limelight, on the front page of news sites like Foreign Policy. The reason for it is not necessarily the most cheerful.

These undersea cables have been under suspected attacks by Russia and China, when speaking of Europe, and Houthi rebels when talking about the Red Sea. However, here at EPIS Europe we are concerned about the seas surrounding our continent, so for now the concern attacks are still looked at from a state actor point of view.

It is necessary to understand that undersea cables are being responsible of 95% of international data, which include diplomatic cables, military communication and of course, financial transactions. It is said that over 10 trillion dollars are being transferred through these cables, representing the backbone of our internet, making them a significant vulnerability for all kinds of other interactions across the globe. All in all, these cables are an issue of Critical Infrastructure.

In their report, Carnegie Endowment for International Peace, raise concerns over the ease with which these cables and their communications can be compromised, and surprisingly, not necessary through the usual sabotage of their cutting. In the policy space of the EU and NATO, serious concerns have been raised over the possibility that these cables could be susceptible to "tapping" as malign actors could compromise their repair process and ultimately install monitoring devices during the rehabilitation process.

Talking of sabotage, what are some concrete examples of such instances? Between 2014 and 2024, Europe experienced a series of undersea infrastructure attacks, predominantly linked to Russia and, to a lesser degree, China. The Baltic Sea became a focal point, beginning with the 2022 sabotage of the Nord Stream pipelines, widely attributed to Russian forces. In November 2024, two key telecommunication cables—BCS East-West Interlink and C-Lion1—were severed off the Finnish coast, with suspicions centering on the Chinese-flagged vessel Yi Peng 3, possibly acting under Russian influence. A month later, an alleged Russian "shadow fleet" oil tanker dragging its anchor damaged the Estlink 2 power cable between Estonia and Finland. These incidents laid bare the vulnerability of Europe's core infrastructure, igniting concern across NATO and the EU.

Looking forward, the purpose of the brief is simply to illustrate the scale and sheer magnitude of the infrastructure we so desperately depend on. With over 1.4 million kilometers of

submarine cables worldwide, the number alone screams for the attention of resilience experts and government worldwide. Each cable represents in the end one step away from a financial shutdown or a missing post day of Elon Musk on X.