Nautical networking

Undersea fiber-optic cables

BY DESSY DUSICHKA, COMPUTER SCIENCE & BIOLOGY, 2025

DESIGN BY VIANNA QUACH, PHARMACEUTICAL SCIENCE, 2025

While it often feels like the internet operates in an invisible "cloud" in the sky, it's actually the opposite — it's powered within the depths of the oceans. Complex hardware underlies all software, and global networking is no exception. The internet relies on submarine fiber-optic cables on the seafloor that form an interconnected highway system for data.

Submarine cables enable everyday communication across the world and support global economies by processing trillions of dollars in daily transactions. Additionally, our networking and data needs are only increasing with the development of new technologies like artificial intelligence, software-as-a-service, and smart devices comprising the Internet of Things. The cables are controlled by individual governments and private corporations, highlighting a lack of centralized regulation over a vital global infrastructure.

The first submarine cables were built in the 1850s using copper to support the telegraph. Today's modern fiber–optic cables contain incredibly thin optical fibers surrounded by layers of protective covering including steel. Currently, over 99% of internet traffic passes through the 870,000–mile network of cables that connect stations on land. There is redundancy within this network, meaning there are multiple routes from one location to another. This is like having additional highway lanes and alternate roads; it ensures there are backup paths for information to travel.

Once cables are installed, they're prone to many threats. The cables are no thicker than a garden hose and can be damaged intentionally or accidentally. There are over 100 instances of submarine cable damage per year, mostly from ship anchors or fishing. Intentional sabotage is also possible since cable locations are public. For example, England cut German telecommunication cables during World War I, and NATO warns of similar attacks in modern warfare.

The network's redundancy serves as its primary protection against these threats. When cables are damaged, alternate routes can usually still carry network traffic, but delays may be introduced (similar to a road detour). Emergency repair teams can also fix damaged cables relatively quickly. If all cables were cut, however, the global internet would no longer exist.

A major challenge in such an international network is determining who has control. Despite the cables being a critical part of today's infrastructure, most nations have not passed legislation to protect them. Making matters more complicated, fiber-optic cables live in the literal murky, gray area between countries. Some nations claim control over the same waters, and some nations don't have any territorial waters at all, meaning they have no control over the cable infrastructure and instead solely rely on other nations with cable landing stations.

> "The cables are controlled by individual governments and private corporations, highlighting a lack of centralized regulation over a vital global infrastructure."

Cable infrastructure involves nations with competing interests, but also includes private stakeholders who may not align with the governments they operate within. For example, Google, Meta, and other big technology corporations have the funds to build and control their own cables. This complicates regulation and raises concerns about net neutrality, since these companies can prioritize their own traffic over other network requests.

The few existing global forums also have limited power. The United Nations Convention on the Law of the Sea is an international treaty asserting that countries are allowed to regulate cables near their own shores and allows any country to establish cables beyond those borders. However, it provides little security and not all nations have ratified it, including the United States. The International Cable Protection Committee is another global forum for discussing technical, legal, and environmental concerns. However, it only gives recommendations, not binding decisions — these decisions are left to individual nations.

Overall, there are risks to digital sovereignty when the cables connecting a nation to the rest of the world are owned and controlled by a different country. This includes the risk of losing internet access itself, but also the risk of data interception through "cable-tapping." The US itself tapped Russian cables in 1970 and has continued to use this technique as recently as 2015, proving that ownership and access to cables provide uniquely powerful intelligence capabilities. Tapping is relatively easy with the right equipment, since patrolling and security the entire network would be a massively expensive undertaking. However, some options for protection include burying cables in trenches for harder identification, and adding sensors to alert cable owners of nearby submarines or potential threats. The sensor strategy is risky though, since it could turn cables into valid military targets and threaten civilian use.

Encrypting data is another way to protect data from cable-tapping by making it virtually unintelligible to anyone reading it. Most data sent over the internet is already encrypted, but not all. This underscores the adoption of secure protocols like HTTPS and integration of encryption services within communication platforms. With the rise of quantum computing, it's possible that even encrypted data could become unencrypted with a powerful enough computer. To combat this, extra-sensitive data can be protected using more advanced quantum-resistant algorithms, which are tougher for computers to decrypt.

While the current network is extensive, new cables are needed to support growing demand. One promising region is the Arctic, which could provide shorter geographic distances than existing east–west cables and reduce delays in network traffic. Additionally, cables can be fitted with environmental sensors to capture ocean and climate change metrics. This would be especially useful in the Arctic, which has been studied much less than other global waters.

Satellites are currently the only infrastructural alternative that work by transmitting data above Earth rather than deep within it. However, they are slower and less widely used (representing only 1% of global internet traffic). Transmitting data openly over the air increases vulnerability to interception and new satellites create additional space debris, potentially harming existing satellites.

The vast web of submarine cables has quietly powered the internet for decades. Strengthening regulations as we expand network capacity will define the future of global communication. The digital world may feel abstract, but its deep-sea backbone remains an infrastructure as vital as it is vulnerable.

Minds and Machines (2024). DOI: 10.1007/s11023-024-09683-z
Science (2023). DOI: 10.1126/science.adi3038
Geographical Review (2020). DOI: 10.1080/00167428.2020.1773266

PHOTOS VIA SHUTTERSTOCK