

Here's how to shut down the internet: Snip undersea fiber-optic cables

December 12 2017, by Tim Johnson, McClatchy Washington Bureau



Credit: CC0 Public Domain

Hundreds of thousands of miles of fiber-optic cable lay on the ocean floors, a crucial part of the global internet's backbone, and only rarely do ship anchors, undersea landslides or saboteurs disrupt them.

Still, a few voices now call for stronger global mechanisms and even military action to protect the cables against future malicious activity by states, saboteurs or extremists.

"The infrastructure that underpins the internet—these undersea cables—are clearly vulnerable," said Rishi Sunak, a British member of Parliament and champion of more vigorous action to protect submarine networks. "They underpin pretty much everything that we do."

Undersea cables conduct nearly 97 percent of all global communications, and every day an estimated \$10 trillion in financial transfers and vast amounts of data pass through the seabed routes. Satellites, once crucial but now limited in speed and bandwidth, handle only a tiny percentage of global communications.

As reliance on the underwater cables soars, a growing list of countries—and even companies—have the expertise to deploy unmanned vehicles to ocean depths to access them.

"Nowadays, there are a lot of countries and companies that have the ability to send vehicles down to the sea floor and have them manipulate, install or take away undersea cables," said Bryan Clark, a retired naval submariner and former Navy strategist who is a senior fellow at the Center for Strategic and Budgetary Assessments, a Washington think tank.

The optical strands inside the cables have extraordinary capacity to transmit data, millions of phone calls per fiber. The cables that house bundled fiber optics are no thicker than a human wrist.

Failures along cable routes are rare, numbering on average barely 200 a year along the estimated 650,000 miles of active international commercial cables laid along sea beds.

"It's still vanishingly small when the amount of cable around the globe is considered," said Keith Schofield, general manager of the International Cable Protection Committee, which has its headquarters in Lymington, England.

There are 428 known commercial fiber-optic cable routes worldwide. Many cables are laid parallel along heavily trafficked routes, like the U.S. to Britain, or through the Mediterranean and Red Sea toward India and the rest of Asia, and come ashore together. Florida has about 10 landing points for the two dozen or so cables that come ashore there.

Most problems occur close to landfall, not in the open ocean, and the majority involve nets from trawlers or damage by anchors, Schofield said.

But in recent years, a few incidents have drawn attention to sabotage and espionage.

In October 2015, U.S. authorities scrambled to monitor Russian submarine patrols and a high-tech Russian surface ship, the Yantar, in a corridor of the North Atlantic that hosts a cluster of undersea cables. The Yantar carried deep-sea submersibles and cable-cutting gear.

In an earlier incident, Egypt said in March 2013 that it had arrested three scuba divers who had tried to cut an undersea fiber optic cable in the Mediterranean off Alexandria that was a vital communications link between Europe, the Middle East and Asia. Egypt never explained who the three saboteurs worked for.

At one time, only the United States and the Soviet Union, now Russia, deployed submarines able to reach deep depths to manipulate [fiber-optic cables](#). But deep-sea remotely powered vehicles are now widely available, putting the technology in more hands.

"All you need to do is give them a claw and sharp jaws and tell them to go down and clip the cable," said Jim Hayes, president of the Fiber Optic Association, a nonprofit professional society based in Santa Monica, California.

Hayes said far simpler means can be found for those intent on damaging the cables, especially near the congested points where they make landfall.

"If you drag an anchor and start pulling with enough force, you can bend and kink the cable ... and snap the fiber," Hayes said.

Since the first submarine telegraphic cable was laid across the Atlantic in 1858, undersea cables have mostly been in private hands, left alone by governments and global bodies.

"Because cables aren't owned by governments, governments have ignored them," Schofield said.

Perhaps not entirely. The U.S. government in the 1970s is known to have tapped a cable off the Kuril Islands in eastern Russia. And in 2013, National Security Agency contractor Edward Snowden revealed that U.S. and British spy agencies were stealing data from undersea cables.

A handful of other nations are believed to have the same capabilities.

Sunak, the British parliamentarian, laid out a number of steps to protect the undersea cables in a 46-page study published Dec. 1 by Britain's Policy Exchange think tank.

He called for enhanced global legal protections, establishing of [cable](#) protection zones above corridors used by multiple [undersea cables](#) and more robust protections at landfall sites.

"They are not secured to the level, for example, of a nuclear power station or a military base is secured at," Sunak said in a telephone interview. "You can find them, sometimes they are just a wire fence and maybe a night-time security guy from the local town. It's not exactly crack security against a terrorist operation."

Sunak's study—Undersea cables: Indispensable, insecure—calls for undersea sensors for cables, creation of backup or "dark" cables that would not be publicly identified, and recognition that an attack on cables would pose "an existential threat" to the world economy.

"We have allowed this vital infrastructure to grow increasingly vulnerable and this should worry us all," former Navy Adm. James Stavridis, former U.S. Supreme Allied Commander in Europe, wrote in a preface to the study.

Others involved in senior U.S. cybersecurity positions concur.

"What it means is that concerned nations need to have robust capabilities to monitor those cables and to repair them or to separate any illegal intrusions," Rand Beers, a former undersecretary of Homeland Security in the Obama administration, said in an interview.

©2017 McClatchy Washington Bureau
Distributed by Tribune Content Agency, LLC.

Citation: Here's how to shut down the internet: Snip undersea fiber-optic cables (2017, December 12) retrieved 26 April 2024 from <https://phys.org/news/2017-12-internet-snip-undersea-fiber-optic-cables.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.