one earth FUTURE
Peace Through Governance

STABLE SEAS
*a program of **One Earth Future***

FACT SHEET | MARCH 2019

THREATS FROM BELOW:
UNDERSEA FIBER-OPTIC CABLE CRITICALITY

by John Filitz

While the maritime security community often focuses on piracy and trafficking, one of the gravest vulnerabilities exists under the surface. More cost-effective and widely used than satellites, critical undersea fiber-optic cable networks are among the most important communication infrastructures globally. Despite the importance of these networks, they receive disproportionately little attention from authorities.

UNDERSEA FIBER-OPTIC CABLES
ARE RESPONSIBLE FOR TRANSMITTING:

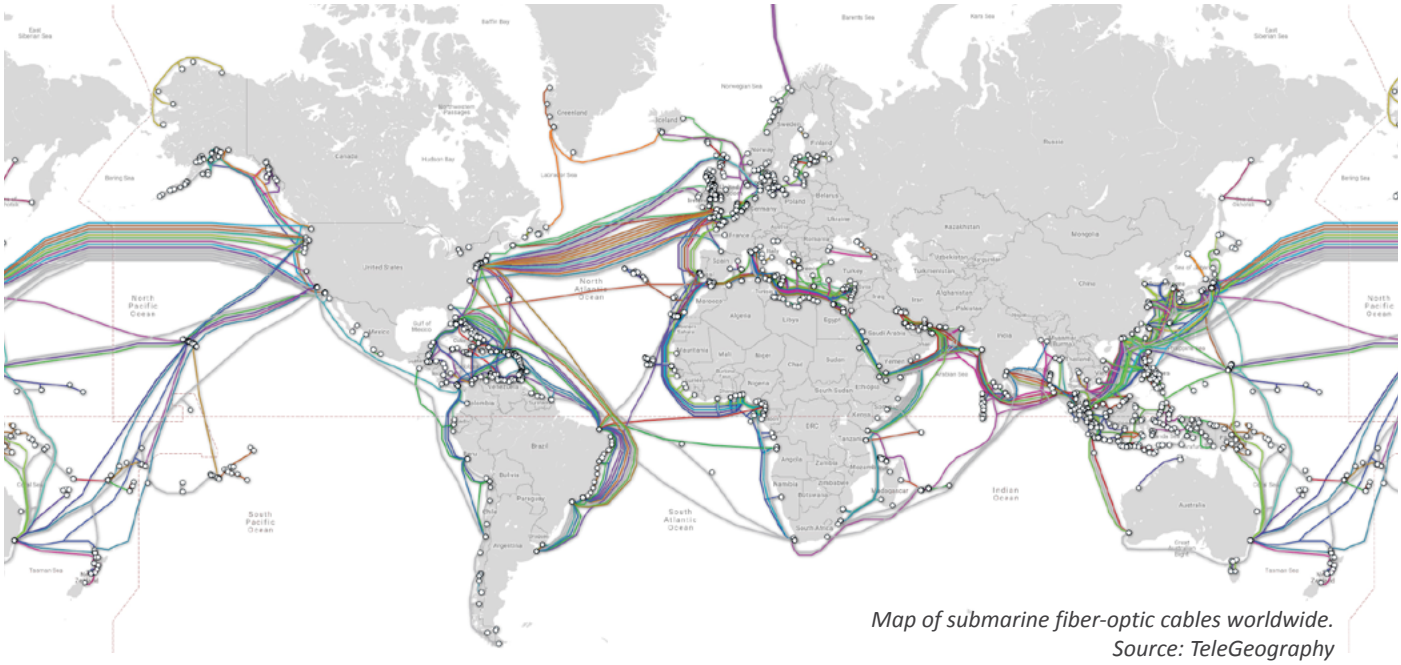
97%
INTERCONTINENTAL COMMUNICATION

15 MILLION+
FINANCIAL TRANSACTIONS DAILY, WORTH
$10 TRILLION

SENSITIVE
& NON-SENSITIVE DATA, AND VOICE CALLS BETWEEN
CONTINENTS & COUNTRIES

UNDERSEA FIBER-OPTIC CABLE NETWORKS ARE THE BACKBONE OF THE GLOBAL ECONOMY:[1]

- More than **200 PRIVATE OPERATORS** control a network of **550,000 MILES** of undersea fiber-optic cable.
- Undersea fiber-optic cables are responsible for **97 PERCENT OF INTERCONTINENTAL COMMUNICATION**.
- Over **15 MILLION FINANCIAL TRANSACTIONS WORTH $10 TRILLION** are facilitated by undersea fiber-optic cables daily.
- **SENSITIVE AND NON-SENSITIVE DATA** and voice calls are transmitted between continents and countries.
- Undersea fiber optic cables have a **LIFESPAN OF 25 YEARS**.
- Inactive cables are called **"DARK CABLES."**
- Several new cross-continental undersea fiber-optic projects are underway **PROMISING SIGNIFICANTLY FASTER INTERNET** in the near future, including the undersea cable currently under construction between Hong Kong and Los Angeles which promises delivery of 144,000 gigabits in 1 second.[2]



Map of submarine fiber-optic cables worldwide.
Source: TeleGeography

RISKS FACING UNDERSEA FIBER-OPTIC CABLES

Undersea fiber-optic cables have a high level of resilience to design, implementation, or configuration flaws. The most significant risks arise due to natural disasters, accidental damage, or malicious interference.[3]

ACCIDENTAL & NATURAL DAMAGE

- Fishing vessels,
- Dredging,
- Anchor dragging,
- Extreme seismic & weather events

MALICIOUS DAMAGE:

- Cyberattacks,
- State and non-state actor sabotage,
- Cable cutting,
- Vandalism and theft

Accidental damage presents the **GREATEST HISTORICAL THREAT** to undersea fiber-optic cables, with numerous incidents of anchor dragging by vessels damaging or severing communication cables.

- The most recent case occurred off the UK island of Jersey in 2016, resulting in significantly reduced internet speeds to and from the island.
- One of the more disruptive incidents took place off the Egyptian coast in 2008:
  - Two civilian ships laid anchor in bad weather, subsequently severing five cables that connected Europe, North Africa, and the Middle East.
  - Internet was disrupted to 80 million people; Egypt and Pakistan lost 70 percent of their internet and India lost 50–60 percent of their westbound internet connection.[4]

Cyberattacks are **INCREASINGLY IDENTIFIED AS THE LEADING THREAT** to the integrity of undersea fiber-optic cable networks. Compromise can manifest as illegal data acquisition for purposes of espionage or criminality, or through disruption or sabotage.[5]

- Given the need for full disclosure to prevent accidental damage by commercial vessels, locations of cables and landing sites are clearly demarcated on maritime maps, making site identification easy.
- Vulnerabilities for intrusion are particularly high at cable landing sites, due in part to significant variability in the level of physical security at landing sites across countries and cable operators.
- Hackers can gain access to, or control over, data and voice traffic either through breaching terminals in cable landing sites or by accessing the data and voice traffic by eavesdropping on/intercepting the fiber-optic wavelengths.

- Other cyber risks include the malicious use of network management systems (NMS), usually used by undersea communication operators to manage the data being transmitted by the cables: [6]
  - NMS are web-based systems relying on readily exploitable HTTP and TCP/IP protocols and Windows operating systems, making these systems extremely vulnerable to comprise.
  - Once a hacker is able to gain access to an NMS, the hacker will have a full access to all data being transmitted in the network and will be able to delete, disrupt, or shut down the data flow at will.

MITIGATION OF RISK:

To mitigate risk of **ACCIDENTAL DAMAGE** to undersea fiber-optic cable requires:

- Burying cables at least 2–6 feet below surface;
- Monitoring for extreme weather events and seismic activity;

For **MALICIOUS DAMAGE** risk mitigation requires:

- Improving the monitoring of data transmission to detect possible interference;
- Improving the physical security of cable landing sites and monitoring of cables in territorial waters;
- Additionally, there is a need to expand the mandate of regional and international cable protection associations to include aspects of malicious compromise.

Members of an underwater construction team repair an undersea cable. Photo: Charles E. White, U.S. Navy.

IMPROVING GOVERNANCE OF UNDERSEA FIBER-OPTIC CABLES

The following steps are necessary to improve governance and mitigate the threats to undersea fiber-optic cables:

- **IMPROVING LEGISLATIVE ENFORCEMENT**:
  - The United Nations Convention on the Law of the Sea (UNCLOS) does provide provisions to physically safeguard undersea fiber-optic cables; however, the provisions are seen as inadequate, particularly concerning the successful prosecution of offenders responsible for malicious compromise.[7]
- **EXPANDING THE MANDATE FOR EXISTING PUBLIC AND PRIVATE INDUSTRY ASSOCIATIONS** will improve the resilience of existing cable network infrastructure from malicious compromise.
- At the country level, steps to improve the disaster and risk resilience of fiber-optic cable networks should include:
  - **CONDUCTING NATIONAL RISK APPRAISALS** concerning the vulnerability of fiber-optic cable network availability;
  - designating cable landing sites as **KEY NATIONAL SECURITY SITES**;
  - business continuity and disaster-resilience **PREPAREDNESS AND TRAINING SHOULD BE ROUTINELY CONDUCTED**: this includes redundancy provisioning of dark cables and network bandwidth for emergency purposes;
  - **IMPROVEMENT OF CABLE MONITORING** for accidental and malicious compromise through the application of new management and monitoring technologies; and regular due diligence and security assessments conducted on cable network operators, including maintenance teams.

ENDNOTES

1 R. Sunak, "Undersea Cables: Indispensable, Insecure," Policy Exchange, December 1, 2017, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf.

2 J. Hecht, "Submarine Cable Goes for Record: 144,000 Gigabits from Hong Kong to L.A. in 1 Second," ITU News, January 5, 2018, https://news.itu.int/submarine-cable-hk-la/.

3 Office of the Director of National Intelligence, "Threats to Undersea Cable Communications," Public-Private Analytic Exchange Program (AEP), September 28, 2017, https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf.

4 Sunak, "Undersea Cables," https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf.

5 M. Sechrist, "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems," Harvard Kennedy School: Belfer Center for Science and International Affairs, 2012, https://www.belfercenter.org/publication/new-threats-old-technology-vulnerabilities-undersea-communication-cable-network.

6 M. Sechrist, "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems," Harvard Kennedy School: Belfer Center for Science and International Affairs, 2012, https://www.belfercenter.org/publication/new-threats-old-technology-vulnerabilities-undersea-communication-cable-network.

7 Sunak, "Undersea Cables," https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf.

STABLE SEAS

a program of ***One Earth Future***

stableseas.org

one earth FUTURE

Peace Through Governance

oneearthfuture.org

+1.303.533.1715 • *stableseas@oneearthfuture.org* • *525 Zang St, Suite C* • *Broomfield, Colorado 80021, USA*