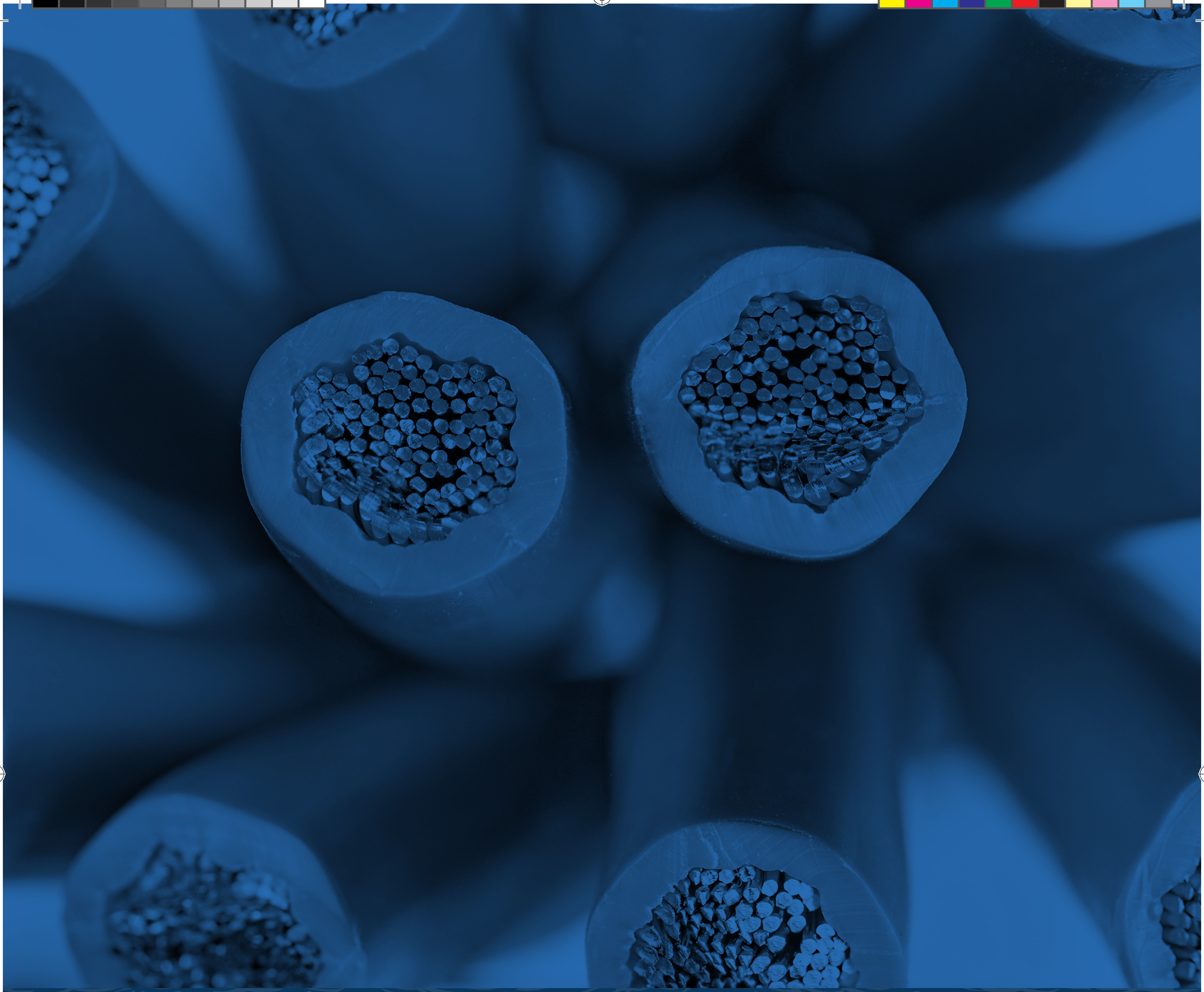


THREATS TO UNDERSEA CABLE COMMUNICATIONS

SEPTEMBER 28, 2017

Threats to Undersea Cable Communications

September 28

2017

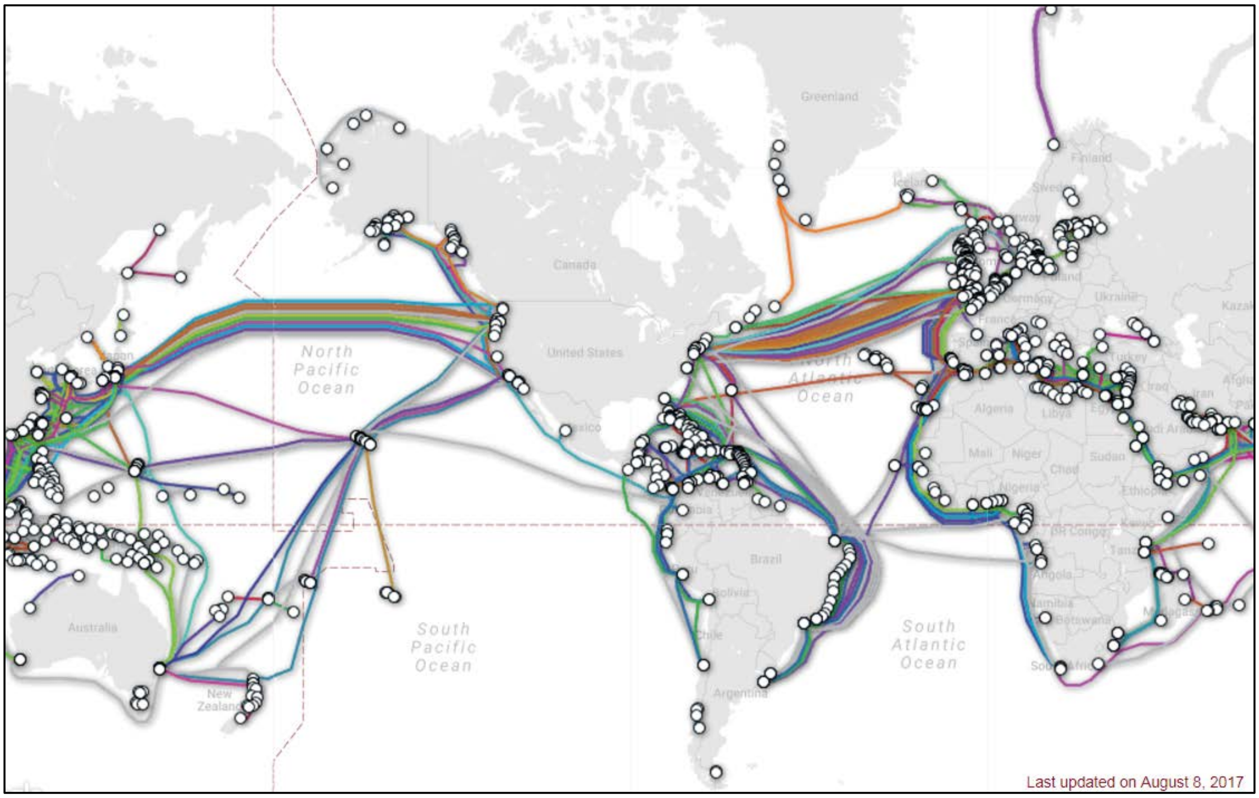
Commercial undersea cable communications carry over 97% of all intercontinental electronic communications, facilitating the reach and speed of internet and phone access critical to international trade, official government communications, and daily end user requirements. This vast, critical submarine network infrastructure remains largely unknown to consumers and corporations not directly affiliated with its development and/or maintenance. However, it is susceptible to damage or destruction by accidental and malicious threats, which can lead to costly, widespread internet and communications disruptions.

This paper is a joint public-private sector analytical product with two primary goals. The first is to highlight potential risks, which could degrade or interrupt submarine cable-supported services. The second goal is to explore collaboration avenues between the United States Government (USG) and the private sector to mitigate threats against domestic cable communications and ensure business continuity.

Examining Strategies Public and Private Entities Can Pursue to Contain Such Threats

2017 PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Global Submarine Cable Network[ii]



Last updated on August 8, 2017

Cable Laying[iii]

Table of Contents

Methodology

Department of Homeland Security Analyst Exchange Program

The Public-Private Analytic Exchange Program (AEP), sponsored by the Department of Homeland Security's Office of Intelligence and Analysis (DHS/I&A), on behalf of the Office of the Director of National Intelligence (ODNI), facilitates collaborative partnerships between members of the intelligence community and private sector industry experts to explore key national security issues in greater depth. Teams work together over a six-month period on a range of important topics to gain a better understanding of how different, yet complementary perspectives and interests, can work in tandem to ensure mission success.

Team Members

The AEP "Threats to Undersea Cable Communications" Team was comprised of public and private sector employees with a range of insights and responsibilities relevant to telecommunications infrastructure. The following team members collaborated and contributed to the creation of this whitepaper:

- James Dean –TrueCourse Advisory Services, LLC
- Shannon N. –Federal Bureau of Investigation
- Donna H. –United States Government
- Michael Marshall –British Telecommunication
- Scott S. –United States Government
- Hubert C. B. –Department of Homeland Security
- Audrey Villinger –Security Industry Specialists, Inc.
- Teyloure Ring – A.S. Solutions
- Heather Nelson –Office of the Director of National Intelligence
- Michael T. –Office of the Director of National Intelligence

Approach

From February through September 2017, the team conducted an independent assessment of the threats to undersea cable communications (UCC) with two primary objectives:

1) Examining vulnerabilities to the undersea cable communications infrastructure, and

2) Developing security risk mitigation strategy considerations for senior leadership of businesses, local, state, and USG personnel who work in the undersea cable communications industry.

Of note, the team used “undersea” and “submarine” interchangeably.

The group communicated weekly and researched various open-source articles, academic journals, and government reports, in addition to holding telephone and in-person interviews with submarine cable subject matter experts (SME), individuals associated with telecommunication entities, and state and federal government agencies focused on or interested in maritime threats. The team also visited cable landing stations and interviewed subject matter experts at a large data center/network access point (NAP).

The work was guided by key intelligence questions (KIQs) developed by the group and a set of carefully considered methodologies. The information provided is not intended to be an exhaustive list of organizational and human factors posing threats to the submarine cable infrastructure. Rather, it is intended to provide the reader a baseline to begin thinking critically about the risks to undersea cable communications and its supporting infrastructure.

Every reasonable effort has been taken to ensure the information and analysis contained in this report were from reliable and reputable sources and that relevant information has been communicated. However, DHS, ODNI, and the AEP team members are not responsible for inaccurate open-source information, including information found in social media outlets, public venues, and public records. Cited information and photo-captured descriptions do not reflect the opinion of any of the above-mentioned parties, but are included to contextualize the analysis.

To protect the confidentiality of information from private- and public-sector contributors, the team conducted interviews on a non-attribution basis and anonymized government agencies, corporate entities, and individuals contacted during this study.

Classification Level

This report is an open-source, unclassified document. In the spirit of AEP’s educational and collaborative mission, redistribution, retransmission, and republication of this report is encouraged.

Introduction

> "When communications networks go down, the financial services sector does not grind to a halt, rather it snaps to a halt."[iv]
>
> Stephen Malphrus, Former Chief of Staff, Federal Reserve Board
> ROGUCCI conference, Dubai, U.A.E., October 19, 2009

This unclassified source study explores the vulnerabilities, risk factors, and disruption indicators within the submarine cable network and supporting infrastructure with the intent of hardening the industry's security measures, improving business continuity, and ultimately reducing operational cost. Focusing on foreign, physical, and insider threats, this report is intended to inform small to medium-sized users (business community and government) and law enforcement personnel of potential security risks and mitigation strategies they may employ or support.

Overall, the overseas communication industry has built-in resiliency for regular, standard, operational single point cable failures. However, a serious simultaneous, multi-occurrence event, be it natural, accidental or malicious could have serious consequences for U.S. businesses and government entities, including the national financial system. Many of these organizations may not be aware of the threat and, therefore, may have no mitigation or business continuity plans in the case of such events.

This study aims to foster greater discussion between private and public entities to educate the community to increase their resiliency.

Critical Findings & Recommendations

The Resilience of the Undersea Cable Communication Network

- Submarine cable networks experience few disruptions in proportion to their heavy distribution throughout the world.
- There have been very limited reports of undersea cable attacks. Terrestrial portions of cable networks are more vulnerable and have been more actively targeted (e.g. The SAM-1 cable across Argentina).
- The majority of undersea cable disruptions are caused by accidents (e.g. fishing nets, dredging, dragging anchor) and natural events (e.g. earthquakes, tsunamis, submarine avalanches, scraping against irregular ocean floor terrain, sharks). For

increased protection, cables near shore are trenched into the ground approximately two to six feet deep, depending on the environment and bottom soil composition.

- Through automated detection, signal re-routing, robust physical and logical redundancy, and a network of repair ships, undersea cable networks have a high degree of resilience from a single-point-of-failure perspective. Numerous and simultaneous cable faults (e.g. caused by natural disaster or targeted attack) can lead to significant service disruption or lags before full restoration is possible.

Conceptual Submarine Cable Segment Threat Matrix

The following table, developed by the AEP team, illustrates the various types of threats which may affect submarine cables to varying degrees, depending on their depths as they traverse the ocean floors to worldwide landing stations.

[Threat Impact Legend: Green = Low; Yellow = Medium; Red = High][1]

2017 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM ***Threats***	***Overland & Last Mile***	***Near-Shore ~130ft***	***Off-Shore 130 - 300ft***	***Continental Shelf 300 - 600 ft***	***Deep Sea ~600 ft +***
Natural					
Sharks	🟩	🟩	🟨	🟨	🟩
Earthquake	🟩	🟨	🟨	🟥	🟥
Landslide	🟩	🟩	🟩	🟥	🟥
Volcano	🟥	🟥	🟩	🟥	🟥
Tsunami	🟩	🟥	🟨	🟨	🟨
Accidental					
Fishing	🟩	🟥	🟨	🟩	🟩
Anchor dragging	🟩	🟥	🟨	🟩	🟩
Dredging	🟩	🟥	🟩	🟩	🟩
Malicious					
Cyber Attack	🟥	🟥	🟩	🟩	🟩
Vandalism	🟥	🟥	🟩	🟩	🟩
Activists	🟥	🟥	🟩	🟩	🟩
Theft	🟩	🟥	🟨	🟩	🟩

[1] Table definitions can be found under ANNEX II

Terrorists	🟨	🟥	🟨	🟨	🟩
State-actors	🟩	🟨	🟥	🟥	🟥

Operational Vulnerabilities

- Although the United States has access to a relatively large number of undersea cables, providing communications redundancy and emergency failovers, many small nation states and island nations (including allies) have few cable access points and are, therefore, more vulnerable to attacks or accidents.
    - Due to the international nature of the submarine network, however, foreign cable faults and disruptions may still affect the United States.
- The concentration of cable landing sites in very few physical locations and the relative ease in finding documented cable routes and cable termination points could facilitate the targeting of the submarine cable network by bad actors.
    - Adversaries with access to cargo ships (to drag anchors) or undersea (near-shore) vehicles could mount a simultaneous attack against multiple cables or multiple attacks against a single cable system that could cause serious long-term disruption.
- More attention appears to be paid to the submerged versus the land-connecting portions of the cables. The AEP interviews indicated minimal organized monitoring of the physical near-shore cable paths via patrol vessels, undersea remotely operated vehicles (ROV), or aerial reconnaissance.
- Moreover, because of their business model, landing station and NAP accesses are granted to employees of dozens of different companies, each adhering to its own security clearance processes. These processes may not be aligned across companies, increasing the probability of insider threats.
- The AEP team interviews indicated a lack of proactive communication across federal and local law enforcement, United States Coast Guard (USCG), telecommunications operators, and landing station operators in coordinating emergency preparedness planning.
- Few businesses dependent on international internet activity seem aware of recovery resources, communication process, or contractual obligations they would be subject to in the event of a serious outage.

Study Recommendations

<u>Private Sector</u>

1) In addition to reviewing their individual policies, operators of cable services should regularly review the security background check policies and procedures of third-

party vendors and sub-contractors to ensure best practice compliance and quality assurance continuity.

2) Small and medium-sized businesses, as well as local and state governments should assess dependencies on international communications and those of third-party vendors, to determine whether disruptions to cable communications would impact their critical operations.
    a. If so, business continuity plans should include:
        i. Identifying critical systems depending on international operations;
        ii. Considering communication contracts with multiple cable operators;
        iii. Examining their contracts with cable operators to understand risks and offered mitigation services;
        iv. Discussing financial mitigation measures with insurance carriers and brokers to determine coverage;
        v. Implementing agreements with satellite communications firms for limited access during an event.

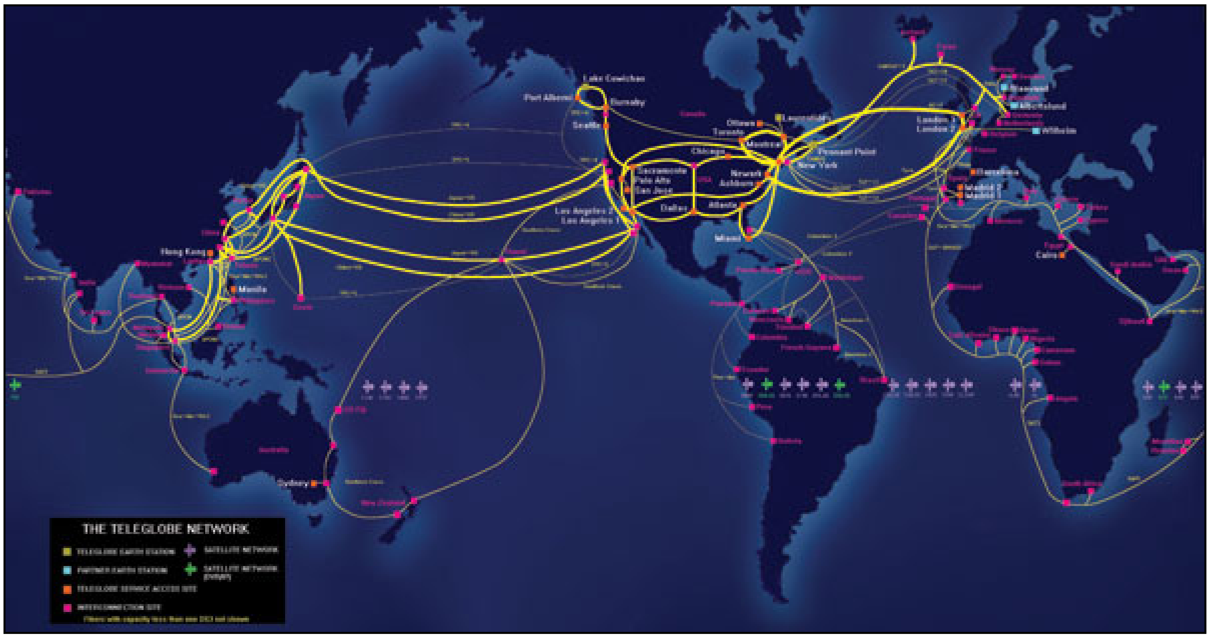
Public & Private Sector

3) Operators of cable services should work with local governments to improve station-to-shore security (such as easing regulations that limit the ability to lock or weld manhole covers).

4) Regional private-public information sharing groups, similar to Information Sharing and Analysis Centers (ISACs) should be established to proactively review risks, coordinate mitigation strategies, and share actionable intelligence. Within the United States, members should include, but not be limited to: Department of Homeland Security (DHS), USCG, Federal Bureau of Investigations (FBI), local law enforcement, telecommunications firms, landing station operators, and undersea cable repair operators.
    a. This study prompted the Southeast Florida Fusion Center to discuss creating such a group with the FBI, and as of the writing of this report those discussions were underway.

5) Local governments should consider establishing community outreach programs (perhaps through FBI InfraGard chapters) to encourage small and medium businesses to assess their risk profiles during significant telecommunications/internet outages and to develop business continuity plans.

The TeleGlobe Network, a Tier 1 internet Service Provider[v]



Foreign Threats

> “If the world’s 223 international undersea cable systems were to suddenly disappear, only a minuscule amount of this traffic would be backed up by satellite, and the internet would effectively be split between continents.”[vi]
>
> Nicole Starosielski, *The Undersea Network*

Overview

The international nature of the submarine cable network, while providing tremendous commercial opportunity, can also create and exacerbate risks to business operations. According to the AEP team’s research, this is in part due to the following characteristics of the undersea cable industry:

- Highly integrated internationally
- International cable network complexity and lack of awareness by risk managers
- Variable levels of resiliency and redundancy across the international network
- Dynamic, with ongoing mergers and acquisitions
- Affected by laws and policies, which vary by country
- Affected by increasing global risk levels
- A single technological point of failure

Submarine cable networks span considerable distances, physically connecting different countries and continents. Every country must rely on submarine cables vital to government, financial, and other business functions. For example, millions of Society for Worldwide International Financial Telecommunications (SWIFT) messages are routinely sent to over 8,300 banking and securities institutions in more than 200 countries. Additionally, the United States Clearing House Interbank Payment System (U.S. CHIPS) processes over one trillion U.S. dollars per day to more than 22 countries for banks, exchanges, and other financial institutions via undersea cables.[vii] These international connections over fiber-optic cables mean that cable disruptions can potentially affect multiple countries and lead to cascading issues internationally, making the point of threat origination more difficult to detect and address.

Aside from physical threats, vulnerabilities may also come in the form of cyber threats via malware from cybercriminals, cyberterrorists, hacktivists, or nation-state adversaries targeting NAP facilities. Whether malicious activities are from lone-wolf actors or from government-sponsored activities attempting to capitalize on an asymmetric advantage, more questions are now being asked related to these international links and the equipment connecting them.

An internationally integrated industry

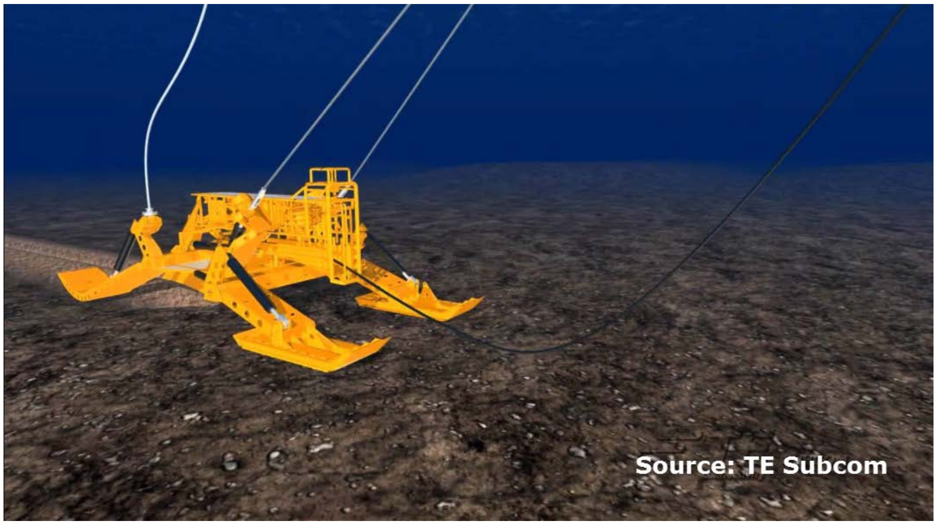
Cable systems are, by their nature, created by international conglomerates; a single cable deployment can represent a $1 billion dollar investment. Therefore, risk and financing are shared among many service providers representing different nations to construct the system. And, when complete, many subcontractors are typically involved with cable operations and repair.

A brief survey of major corporate players in the submarine cable industry reveals an extensive list of companies from diverse countries. Companies around the world can gain the expertise necessary to be dominant market players in various aspects of the cable system, including research and development, manufacturing, installation, maintenance, testing, and repair. Some of these companies operate globally, while others concentrate their expertise and operations in one or two regions.

There are now four oceanic cable suppliers: Nokia-Alcatel, which continues manufacturing in France and the United Kingdom, but is now under Finnish ownership; TE-Subcom which maintains many United States based operations, but is under Swiss ownership; NEC from Japan; and Huawei Marine from China.[viii] Over the past five years, all four of these companies have been responsible for the installation of thirty-nine cable systems:[ix]

- Alcatel Submarine Networks (ASN, now Nokia-Alcatel) – 17 systems
- NEC – 9 systems
- TE-Subcom – 8 systems
- Huawei Marine – 5 systems

Submerged Plough Burying Undersea Cable[x]



Source: TE Subcom

The optical networking (terminal equipment) industry in undersea cable communications is international as well. Some of the major players in existing and newly upgraded systems include Ciena (U.S.), TE-Subcom (U.S.), ASN (France/Finland), Mitsubishi Electric (Japan), Fujitsu (Japan), NEC (Japan), and Huawei (China).

The global nature of the undersea cable industry entails remarkable cooperation levels; however, it can also hinder basic industry necessities such as timely cable repair. For example, before the cables are laid, surveys must be conducted and cable repair agreements penned. The latter may be zone agreements like the Atlantic Cable Maintenance Agreement (ACMA) or Mediterranean Cable Maintenance Agreement (MECMA); or private agreements such as the Atlantic Private Maintenance Agreement (APMA) or North Pacific Marine Maintenance Service Agreement (NPMMSA). These repair agreements can encompass international companies and cable repair ships that are mostly foreign-flagged and moored at foreign ports. These factors in turn can lead to delays resulting from problems related to distance, weather conditions, and repair prioritization. Also, although, internationally, spare cable repair equipment is often stored near cable sites to provide better business continuity, there is no universal equipment database providing rapid insight into the closest, necessary product if locally stored resources are insufficient. Furthermore, natural disasters or political situations in countries handling cable issues or providing spare parts may affect the speed of cable repair time, which is generally first come first served, or highest payer first (according to the length of the cable).

From a communications standpoint, Network Operations Centers (NOC), which monitor security threats to the cable network, may be based in a foreign country, selected for geographical operational stability and cost-saving properties. However, legal, cultural, and language barriers may limit the ease and effectiveness of information flow in the event of a disruption, and depending on where cable disruption symptoms appear, public agencies without a local presence may struggle to coordinate a timely response.

Industry dynamics

Business fluctuations in this dynamic industry pose a security practice continuity challenge which may not be fully appreciated by all companies reliant on cable communications. The industry is constantly changing, as companies merge or change ownership in efforts to reduce cost and become more competitive. Other companies have been forced out of business or taken over due to extreme competition.

In January 2016, Alcatel-Lucent completed its merger with Nokia, which began in April 2015. British company Xtera filed for Chapter 11 bankruptcy in 2016, and Miami-based private equity investment firm H.I.G. Capital acquired the assets.[xi] United States based Hybernia was also bought out in January 2017 by United States based GTT Communications.

An increasingly complex system

Submarine cable systems are often cited as carrying 97% or more of global data traffic. The amount of information constantly passing over these systems is daunting. Average system capacity in 2014 was approximately 20 Tbps, while in 2017 it is over 60 Tbps.[xii] Most upgraded systems today transmit 100GBps over a single wavelength, and are operating 30 or more wavelengths on a single fiber pair. Today, there are about sixteen transatlantic cable systems and eighteen transpacific cable systems currently in operation or under development, and in total, there are over 250 separate submarine cable networks operating or under construction totaling over approximately 550,000 miles of fiber-optic cable.[xiii]

Increasing risks to undersea cables

Possibly due to the relatively discreet nature of submarine cable communications, the industry has suffered remarkably few issues since its inception nearly 150 years ago.

Fortunately for actors wishing to disrupt cable systems, the public has a general lack of awareness of the scope and criticality of the vast array of submarine cable systems.

In 2013, the South East Asia-Middle East-Western-Europe 4 (SMW 4) cable was intentionally cut by a diver, crippling internet speeds by 60% in Egypt. In this instance, the damage caused internet slowdowns for all service providers, and took around 20 hours to resolve.[xiv] In 2007, Vietnamese pirates stole optical amplifiers which left a cable system inoperative for 79 days. Scenarios such as these coupled with the growing global dependency on telecommunications are gradually forcing the subject of modern submarine cable systems risks into public consciousness, but few appreciate its scope.

John Tibbles highlighted in an article in May 2017 the changes in the technological and political landscape that could lead to increased potential for a mini or cyber cold war, new competition in the Arctic Ocean, and other factors that could lead to increased threats to the United States' cable systems stemming from state-sponsored cyber-attacks.[xv]

One method to help explain the risk to critical telecommunications infrastructure is using a danger index.

Danger = Intention x Capability x Vulnerability x Consequence[xvi]

If the risk to undersea cable customers can be described as the product of potential intent and capability by malicious actors, vulnerability to intentional or unintentional disruption, and the magnitude of potential consequences, this risk has steadily risen since the inception of fiber-optic undersea cables in the early 2000s. Some of the causal factors for this progressive uptick include:[xvii]

- Market share fluctuations and industry evolution has reorganized the economic balance of power. Where the United States and other western companies used to be dominant manufacturers, Asia now dominates in many respects.
- The amount of data traversing transoceanic cables is many times what it was a few years ago and constantly rising.[xviii] Moreover, the widespread use of cloud storage by the banking and government sectors, among others, suggests that any major cable disruption would cause an unprecedented degree of communication failure.
- Cable systems are now much more vulnerable due to the nature of modern, remotely controlled network management systems. Equipment such as Reconfigurable Optical Add/Drop multiplexers (ROADM) can be manipulated from afar, such that malicious activity could physically change a network or drop communication paths altogether.[xix]

- Terrorist networks are becoming more sophisticated and international. Although terrorists also heavily rely on virtual communications, their nihilistic mindset may cause them to reach a risk/reward calculus in favor of disruption.
- Indications of increased willingness and capability for cyber activity and cyberspace attacks by nation-state adversaries on specific industries (e.g. see media reporting regarding the Sony hacks).
- Open-source news stories indicate some governments and corporations are becoming more concerned about a foreign nation state's ability to interfere with a submarine cable system. For example, Australia intends to halt construction of a planned 2,485 miles (4,000 kilometer) submarine cable system due to the government of the Solomon Island's decision to change original plans with another firm and begin pursuing an opaque deal with Huawei in mid-2016.[xx]

Laws and policies vary by country

Many countries lack legislation criminalizing the theft and destruction of undersea cable infrastructure. Laws in the UK and Australia vary from those of the United States, which in turn vary from South America, Asia, and Africa. For instance, all beach manholes in Brazil are required to be tack-welded shut, while this is not a common practice in the United States. Inconsistency such as this presents a potential physical security vulnerability. Australia and New Zealand, very likely due to their total reliance on undersea cable networks for connectivity to the rest of the world, have very advanced cable protection regimes, which include established cable protection zones and corridors,[xxi] enforced by air and sea patrols. Additionally, civil and criminal liability and potential financial penalties for causing cable damage in Australia can be extremely high. In contrast, the United States' financial penalty amounts have not been updated in over 125 years and therefore do not serve as effective deterrents to cable damage.

These differences in approach have been highlighted by organizations like the Council for Security Cooperation in the Asia Pacific (CSCAP), which published a 2014 report highlighting recommendations to better align and improve outdated laws and policies to address intentional damage caused by terrorists or others.[xxii]

Moreover, the AEP team's discussion with the Miami-Dade Police Department Southeast Florida Fusion Center underlined the jurisdictional overlap submarine cables present once they make landfall. Rather than providing redundant security mitigation practices and oversight bodies, the overlap, at least in the United States, can lead to heavy reliance on the private sector to audit security practices and those of their supporting vendors and companies. Additionally, all entities involved may be under the erroneous assumption that other agencies are engaging with the private sector around security concerns, potentially leading to shortfalls.

Knowledge is power

Within the submarine cable communications industry itself, no single or group of federal agencies is dedicated to fielding company questions around vendor, supplier, contractor, and manufacturer resources; investigating flagged issues (e.g. unusual observed maritime activity); and/or facilitating issue resolution. Although very large customers and consumers are highly aware of submarine cable security factors and the impacts of communication failures, small to medium customers are less so.[xxiii] Large customers will ask detailed questions about the resiliency of their communications services. This may include information on:

- Logical redundancy, such as backup reserved bandwidth and logical communication protection schemes. Most submarine cable systems have at least partially meshed networks, where customers' data and communications travel to two or more destinations. If one link is broken, the other link will take over as the primary link with no loss of information.
- Physical redundancy, such as redundant paths and multiple termination points. A transoceanic cable essentially forms a large ring, with two separate, redundant paths so that a cable fault will not disrupt that cable's communications. In addition, the cable will often branch into two separate cables miles offshore and terminate at two different beach manholes, reducing the risk of cable faults, which most often occur close to shore.
- Service level agreement (SLA) contracts, between customer and service providers, which ensure issues are resolved in a timely and efficient manner, and communicated so businesses can take appropriate response measures.

Smaller customers may ask fewer questions directly related to the submarine cable network or communications resiliency their service includes, assuming it must be dependable. However, as customers become more knowledgeable, grow their customer/shareholder base, or depend more heavily on telecommunications (with larger implications – financial or otherwise), they should ask more detailed questions on the specifics of their service contract.[xxiv]

In interviews with various cable system operators, our team learned that these particular companies have not knowingly experienced cable system disruptions due to vendor selection, international supply chain issues, or cyber-related incidents. Although the cable system operators and large service providers interviewed for this paper have no direct knowledge of current, active threats to their systems, they have a great appreciation for the changes occurring in the industry and the potential for new and increasing threats.

When a U.S. service provider or major telecommunications company is evaluating foreign companies as suppliers for new systems and upgrades, they must ensure these companies are not restricted from U.S. markets. The primary way they do this is through collaboration with the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an interagency committee that includes expertise from the Department of Commerce and the Federal Bureau of Investigation (FBI). CFIUS approves foreign companies' operations in the United States, which may deal with foreign business licenses and purchase of foreign business products.

In this case, foreign governments or foreign service providers may be involved in new or upgraded submarine cable systems or services, and the foreign products could include telecommunications equipment from foreign vendors. If U.S. customers or telecommunications service providers want to use equipment or companies being evaluated by CFIUS, they must obtain approval prior to making these purchases or operations agreements.

Recommendations

- Service providers and customers should be aware of differing international (and sometimes regional) standards; the complexity of cable ownership, which can affect maintenance, responsiveness to repairs, development, and operational transparency.

- Service providers and customers should ensure they conduct due diligence into the various parties involved in the placement, maintenance, and repair of submarine cables as security best practices are not standardized throughout the industry, in the United States, or internationally.

- Customers should know where they stand in the priority queue if multiple cable breaks occur and repair resources are strained.

- Customers and service providers should create or improve their own security review guidelines and requirements and ask questions to better understand the contractors, manufacturers, supply chain operations and limitations, and network resilience requirements for their systems and service contracts.

- U.S. Government liaising or involvement with the private sector regarding submarine cable risks should be improved, particularly in areas of jurisdictional overlap (e.g. landing stations and shallower waters where submarine cables connect with land).

- Active involvement with existing industry forums, partnerships, committees, and governments should be increased. Some of these activities and organizations include:
  - The International Cable Protection Committee (ICPC).
  - The Communications Security Reliability, and Interoperability Council (CSRIC) and associated working groups
  - The North American Submarine Cable Association (NASCA)
  - Committee on Foreign Investment in the United States (CFIUS)
  - U.S. Department of Homeland Security (DHS)

- Government and private-sector entities must cooperate in developing national and international laws to protect undersea cable communications.

Exposed Cable[xxv]

Cable Man-hole[xxvi]

Cable-Entangled Anchor[xxvii]

Submarine Avalanche[xxviii]

Sub-marine Landslide waiting to happen...
Puerto Rico Trench
Dominican Republic
Puerto Rico

Physical Threats

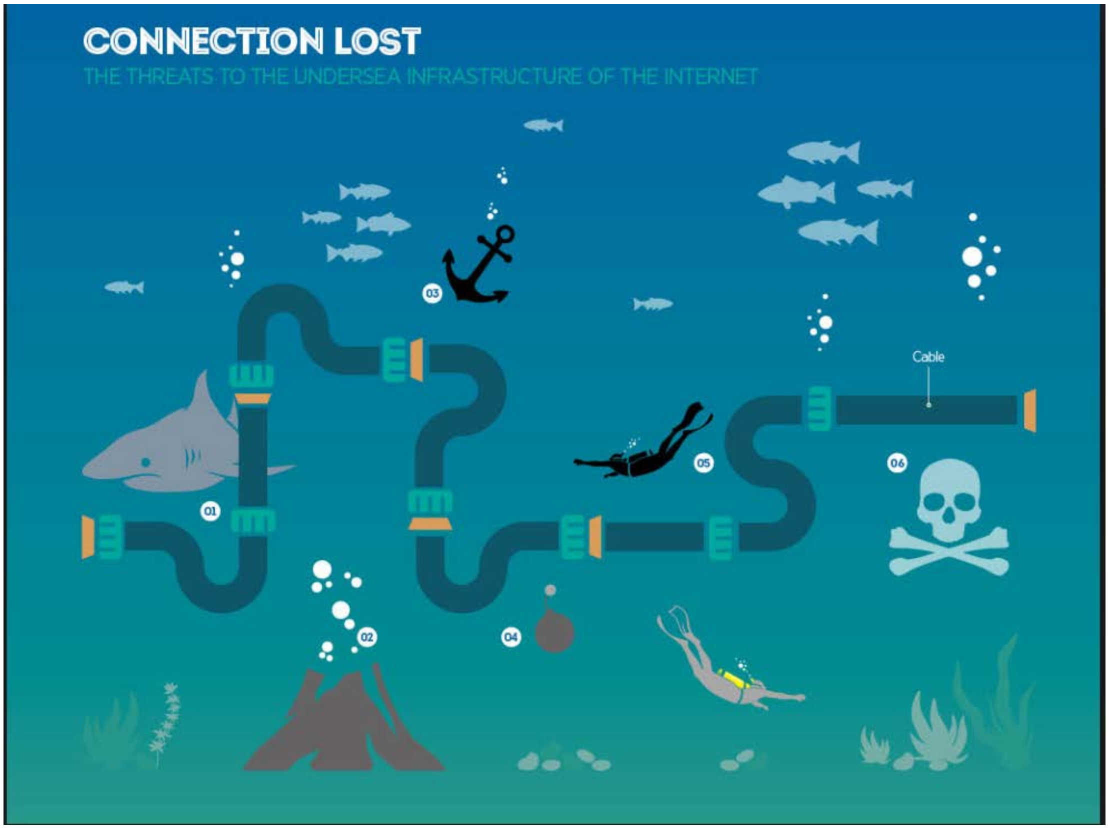
> "Specialist marine engineers have been called in to fix a sub-sea fibre-optic cable damaged by copper cable thieves who couldn't tell the difference… The thieves struck at low tide in Loch Carron last Thursday, and BT engineers had to race to install a temporary cable at low tide the next day."
>
> RECOMBU, 11 June 2012

Overview

As with any network responsible for the transmission of critical data, the need to protect the physical components of the network is at the core of providing a resilient, reliable, consistent and secure data transmission.[xxix] With the global subsea fiber-optic network responsible for 97% of transoceanic internet transmissions, protecting the physical infrastructure of this network is fundamental to delivering the services expected by all internet consumers.

Deliberate physical attacks on the UCC infrastructure have the potential to significantly disrupt the global economy and degrade national security. Within the United States, cable landing stations are the most accessible and impact-rich targets as they are concentrated in a handful of coastal locations. For instance, there is a major concentration of optic cable landings in New York, New Jersey, and Miami on the east coast; and in Seattle, Portland, and Los Angeles on the west coast. Traditional facility and access control measures are used to mitigate threats at the landing sites and landing stations. Still, there is room for increased collaboration across public and private sectors. For example, there are no regulations of ownership for real estate located near landing stations and NAPs.

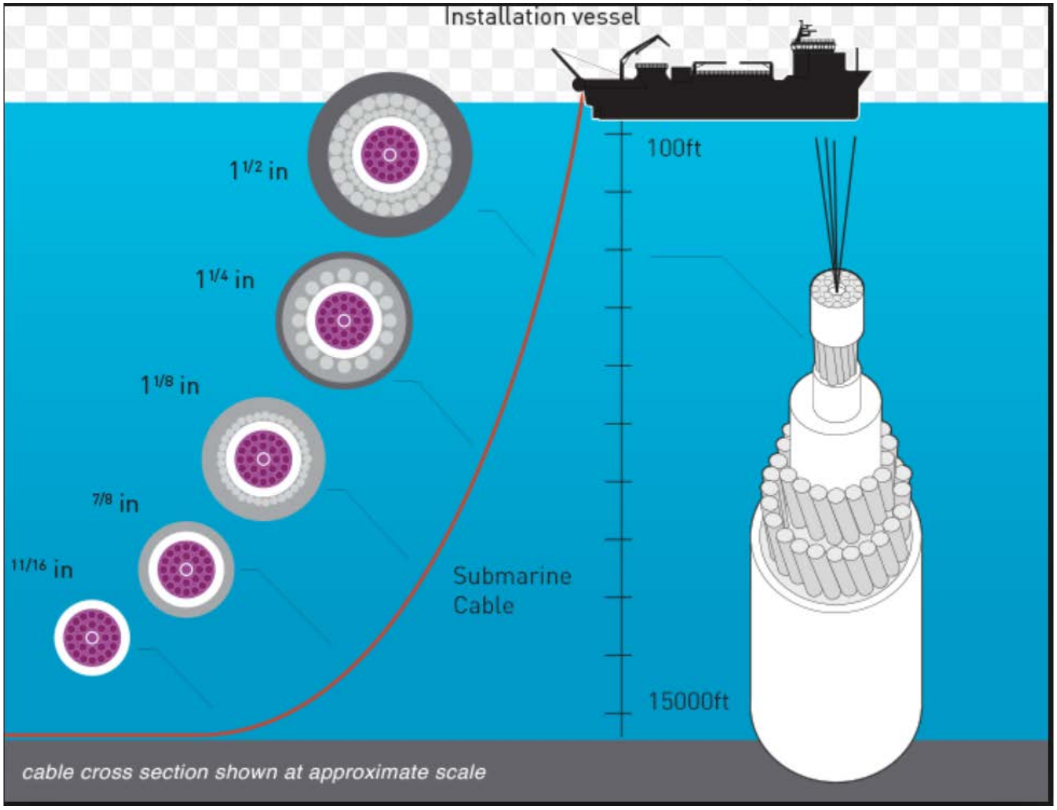
Threats to Undersea internet Infrastructure[xxx]



End-to-end deployment of the subsea cabling can be found in the deep-sea environment, territorial waters, near-shore shallow waters, initial landfall junctions and landing stations (see Annex II), and each segment has its own resiliency challenges. The characteristic of the subsea network is diverse in its physical makeup, components and deployment methods based on the geographical location of the cabling. Example of this diversity can be seen in the circumference of the cabling based on the depth where the cabling is deployed.

Additionally, cable design can differ. For instance, optical amplifiers may be installed between cabling segments, cabling splitters close to shallow waters, and/or cabling junction connectors at the first point of cable landfall to the cabling interfaces at the landing stations. Constant changes in the cabling characteristic calls for a multifaceted approach to protecting the physical infrastructure of the subsea cables.

Cable Cross Sections at Various Depths[xxxi]



For the water-based elements, cables are frequently buried close to shore, offering a layer of protection. And, although cables lie on the seabed in deeper waters, their exact location is not publicly disclosed, making them more difficult to accurately target. However, the practice of "clustering" cables, or locating multiple cables in a small area, has increased the physical vulnerability of the cable systems. For example, attackers could maximize damage by dragging an anchor through a cluster of cables. Cable repair ships are strategically located around the globe for rapid deployment but could also be attacked or impacted by malicious activity.[xxxii]

Threat Vectors

Threats to the physical wellbeing of the subsea cabling can come from multiple threat vectors, including:

- Environmental

    - Deep sea earthquakes and other seismic events have been known to sever or disrupt the subsea cabling integrity.

- Sea Life
    - Video surveillance has captured shark attacks to undersea cable segments and scraping of the cable against rougher sea vegetation and debris can cause damage.

- Accidental and Negligence
    - Damage from dragging of anchors or dredging in swallow waters commonly disrupt subsea cables.

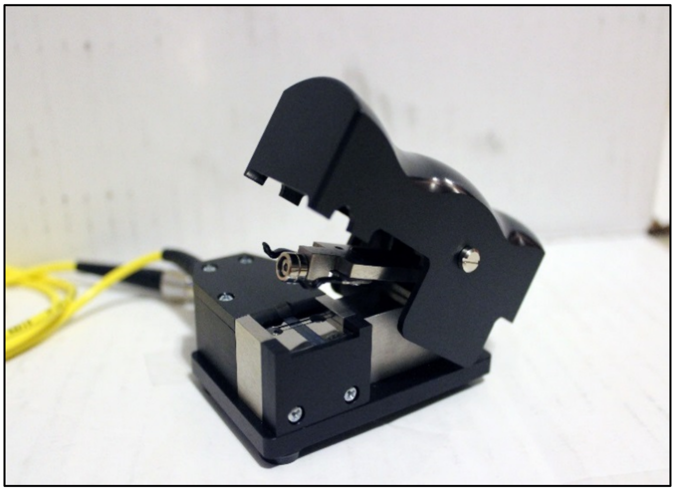
- Intentional Sabotage
    - Creating economic havoc, political discourse and other geopolitical instability can occur with the simple cut of a subsea cable. Coordinated cuts of multiple cables executed in a strategic manner could bring a country or region to a standstill.

Cyber Attack

The technological access and motivation of a malicious actor to successfully “hack” or “sniff” a fiber optic network by tapping secretly into a fiber optic cable, under the water or at a landing station, should be recognized as a capability of cyber-criminal behavior.

As fiber optical networks may have link loss budgets of 14dB or more (equating to 96% signal loss), not all taps are immediately detected. A well designed fiber network can experience a wide variety of anomalies with no data loss or network warnings detected by network monitoring systems.

Fiber-Optic Clip-On Coupler[xxxiii]



Indicators

- **Alarms:** The submarine network relies on embedded alarm and trigger mechanisms, which notify and provide approximate geo-coordinates on where cable damage has been detected, and may indicate the type of damage or interference. Landing stations and NAPs also typically employ access control systems and CCTV camera surveillance, securing sensitive areas such as equipment cages.
- **Outages:** Cut cables, particularly for nation-states with fewer cable connections, can lead to significant internet and telecommunication outages, as seen in the examples cited in “increasing risks to undersea cable” section earlier in the study.

Mitigation Methods

- Traditional facility and access control measures can deter physical threats at landing sites and landing stations.
- Undersea cables are frequently buried in shallow water and their exact locations are identified via public internet access and public maritime charts and charting systems, however in the high seas are not mapped, adding a layer of security.
- If an attack is successful, cable ships are located around the globe ready for rapid deployment.[xxxiv]

Recommendations

- Bury the fiber in concrete where practical and allowed by law, weld shut manhole covers, and secure wiring closet doors, riser access panels, and elevator shafts where network cabling exist.

- Leverage optical time-domain reflectometer (OTDR) tools to help identify, detect and pinpoint physical flaws within the fiber optic network.

- Provide continuous, real-time, and independent data monitoring to detect and identify anomalies, loss of dB, or other indicators of instability. For instance, a loss of signal strength could indicate cable damage or intrusion attempts by malicious actors.

- Build business resiliency programs, which include automated network switch-overs from “suspect” or compromised networks to redundant ones.
  - The strategy of empowering a network monitoring system to “Detect”, “Isolate” and “Re-Route”, during a fiber network incident could minimize the disruption from a network event.

- National, regional, public and private sector stakeholders must develop contingency plans to respond to undersea cable infrastructure disruption.[xxxv]

- Greater outreach is needed by the government to coordinate contingency plans with national, regional and private sector stakeholders in the event of an attack on the undersea cable network.

- Government and private sector entities must work to develop national and international laws criminalizing the destruction of undersea cable infrastructure.

Insider Threat

> *"Insiders pose a substantial threat to your organization because they have the knowledge and access to proprietary systems that allow them to bypass security measures through legitimate means."*[xxxvii]
>
> *CERT, 2017*

Overview

Similar to other technologies, particularly those involving human intelligence factors, undersea cable communications are susceptible to both physical and virtual threats. In recent years, various events have called attention to the risk of threat from an insider. Across the public and private sectors, stories of employees using the access granted to them to steal or alter the information is becoming more common.

For the purposes of this paper, an insider is defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data. While an insider risk is defined as the probability such an individual "will use their authorized access, wittingly or unwittingly, to do harm to their organizations."[xxxviii] Putting these definitions into practice reveals the threat to business and government operations is broad as proprietary systems may provide the insider access to consumer information, intellectual property (IP), or provide them the ability to impair the integrity and availability of data.[xxxix] As such, insider threats must be addressed in a methodical manner.

Risk to Undersea Cable Communications

The team's research indicated that insider threats to UCC were not uppermost in the industry's strategic planning. In fact, on at least two occasions when the AEP team was in dialogue with cable landing station and NAP subject matter experts, these individuals seemed surprised by the notion of insider threats. Their surprise might be attributable to and consistent with the findings that, to date, this has not been a glaring issue for the industry. Nevertheless, the international communications connectedness, which relies primarily on undersea cables,[xl] warrants a closer look at the possible risks to undersea cable communications.[xli]

While the physical security of undersea cables seems less impervious to malicious acts, attacks involving the virtual or cyber aspect of submarine cable systems would entail hacking into the cable network management systems used to operate them and disrupt communications.[xlii] Insiders who merge their advanced technological understanding with traditional espionage or terrorist abilities have significantly increased opportunities to cause physical damage through cyber means.[xliii] Like many other systems, undersea cable communications are dependent on other infrastructures. The landing station environment, for example, is heavily dependent on the people who maintain it and have access to it.[xliv] And, according to the 2010 Reliability of Global Undersea Cable Communications Infrastructure (ROGUCCI) Study and Global Summit Report, while the undersea cable system software managers seem to be fighting the trend to increasingly rely on outsourcing software development, most areas of the Information and Communications Technology (ICT) industry acquire material from outside sources.[xlv]

Furthermore, outsourcing introduces the notion of supply chain insider threats, which is a trend that is of particular interest to businesses everywhere, as demonstrated by the breech of Target's systems through a third-party service provider in 2014.

Government officials and experts on control systems that govern the United States' critical infrastructure expressed increasing concern about potential cyber threats to those control systems.[xlvi] For example, businesses that use Supervisory Control and Data Acquisition

(SCADA) networks inherently have business models without exact boundaries in which an outsider may quickly become an insider by entering through the weakest link (e.g. field networks, vendors, and the supply chain).[xlvii][xlviii]

If a hacker penetrates a cable management system, he or she could gain administrative rights and hack into the presentation server. Presentation servers can host web-based applications for numerous cable operators and handle management system data for multiple cable systems. Hacking into a presentation server can, therefore, provide attackers control of multiple cable management systems, unprecedented top-level visibility of multiple cable networks and data flows, knowledge of physical cable vulnerabilities, and the ability to disrupt and divert traffic. With that access, an attacker may gain a potential "kill click." With a click of a mouse he or she could delete wavelengths and, potentially, significantly disrupt or alter global internet traffic routes.[xlix]

Another aspect of the insider threat consideration to United States interests is the globalization of the undersea cables owners and operators. The majority of countries now rely on submarine cables for their communications needs, and the global submarine network forms the backbone of the Internet.[l] The interdependence nations have for forming consortia to purchase and maintain the cables may also present vulnerabilities, which could be exploited and affect the United States.[li] Research did not clearly determine what persons are in each international NOC or precisely how those employees are vetted. While the companies the AEP team visited all have thorough employee vetting, they only represented a small, national sample size.

Every element involved in supporting UCC such as personnel at the cable landing stations, centralized network management centers, and cable repair entities is susceptible to threats from insiders.[lii] For example, individuals with physical access to a cable landing station have tremendous amounts of access (physical and logical) to equipment that is vital to maintaining undersea cable communications. Equipment housed within these facilities provides the power to the undersea cables and enable the transmission of vast amounts of internet traffic. Individuals with logical access to network management tools (SCADA) also have the ability to disrupt the communications, as mentioned earlier. For these reasons the AEP team recommends businesses that are using, or considering using, undersea cables to transmit data vital for their company's survival, thoroughly understand how the cable providers with whom they are contracting manage the risk from insiders.

Indicators

Some organizational tendencies and behaviors may be indicators of an insider threat.[liii] While these indicators are general and could be applied to many industries, they remain credible and applicable to undersea cable communication operations and personnel. A few organizational factors that may increase the risk of insider threats include:

- A perception that security is lax,
- Access privileges granted to those who don't need it for their job duties, and
- Time pressure to complete responsibilities.[liv]

There are some behavioral tendencies or warning signs that may be used to predict threat from an insider. These include:

- Working odd hours without authorization,
- Unreported foreign contacts and unexplained short trips to foreign countries, and
- Abrupt requests for changes to Supply Chain equipment and service contracts.[lv]

Mitigation Methods

- The private sector has ready access to open source resources to educate themselves and establish an insider threat program.
    - Perhaps one of the most widely recognized authorities on the subject in the U.S. is the CERT Insider Threat Center associated with Carnegie Mellon University,[lvi] whose publicly available "Common Sense Guide to Mitigating Insider Threats" includes 20 practices that organizations should implement to prevent and detect insider threats. Practices include "know and protect your critical assets", "beginning with the hiring process, monitor and respond to suspicious or disruptive behavior", and "consider threats from insiders and business partners in enterprise-wide risk assessments." It includes challenges and quick wins, including references to industry standards such as NIST (National Institute of Standards and Technology).[lvii] NIST was founded in 1901 and is now part of the U.S. Department of Commerce. NIST provides technology and measurement standards for various industries.

- The U.S. Government departments and agencies may leverage the National Insider Threat Task Force (NITTF), which was established under Executive Order 13587, to develop their insider threat program.[lviii] The NITTF mission is to deter, detect and mitigate actions by employees who may represent a threat to national security by developing a national insider threat program.

    - The NITTF guidelines are purposely broad to enable them to be applied across industries and entities. Common themes include engaging the right individuals (with decision making authority) from key organizations, defining what differentiates the organization from others or what makes it a target (Crown Jewels), and determining how it is protected and shared outside of the organization. Furthermore, personnel-related programs must be established to include thorough and periodic background checks, termination checklists and procedures and Non-Disclosure / Non-Compete / Agreements.[lix]

- Considering the various components and infrastructure necessary for the submarine cable network's successful operation (incl. cable landing stations, centralized network management centers, and cable repair entities), a comprehensive insider risk program should be established and managed across all involved parties.

Recommendations

Undersea cable communications are at risk from insider threats and there are mitigation actions that should be discussed and implemented with cable operator cooperation to ensure the integrity of undersea cable communications remains at the highest levels.

- When discussing the use of undersea cables to transmit communications and data, business owners should require potential suppliers to provide an overview of their insider threat program and actions that have been taken to mitigate the risk from insiders. The Request for Proposal (RFP) process is often the best mechanism for requesting and obtaining this information from possible suppliers.

- Cable and data center operators should have established processes for initial and ongoing background checks for employees and contractors. Additionally, termination activities should be clearly documented (e.g. leveraging a checklist) and executed rapidly when a resource exits their position. For example, when an employee leaves the company or moves to a different position within the company, a series of activities should be taken to ensure their physical and logical access is removed from the systems and facilities that will not be needed in their new role. Implementing systems and tools to address Data Loss Prevention (DLP) are highly recommended as the timeframes leading up to an employee's termination and the 30 days following are critical to monitor as it is common for exiting resources to download and take information with them, for reference in future positions or for nefarious activities.

- System access should be periodically reviewed and oversight of those with elevated access or administrative access to SCADA systems should be analyzed for suspicious patterns such as granting others administrative access or access that is beyond what is needed for their job duties, and initiating frequent password changes.
  - Resources should be granted the least amount of access to systems that is needed for them to fulfill their job responsibilities.
  - The level of access should be reviewed by management periodically to ensure it is still warranted.
  - Actions performed by those with elevated or administrative access to systems should be audited regularly to ensure actions are in alignment with their assigned duties.

- Physical access to cable landing stations and locations housing the equipment that operates the undersea cables must be managed and tracked closely.
  - Former employees, contractors, and vendors should not be allowed access to equipment areas.
  - Visitors should be accompanied at all times and their information documented and available for auditing.

- Cable landing station operators, cable repair entities, and data center operators should consider identifying activities that require two resources to complete and sign off, with the two resources being peers or manager/subordinate. Actions that can be performed by a single resource with no oversight or engagement with others may provide the resource undue power and authority which can lead to increased risk to operations.

Conclusion

Although a significant body of work has been done on this topic, it has largely been confined to the intelligence community, the military, and the undersea telecommunications industry. It became apparent from the AEP interviews conducted that many end users of these services (especially small, medium sized organizations and local and state governments) are not well-informed on the vulnerabilities of the multi-faceted undersea cable network. Yet, these organizations are dependent on international communications more than ever before.

This product may assist end users and risk managers in gaining a more in-depth understanding of the vulnerabilities associated with the use of undersea cable services, therefore strengthening mitigation and business continuity efforts in case of a significant disruption. Exercising the recommendations in this paper through a private-public effort, may increase the resiliency of the economy and ultimately enhance national security.

---------- End of Paper -----------

ANNEX I - Lexicon

Bandwidth: The capacity of a telecom line to carry signals. The necessary bandwidth is the amount of spectrum required to transmit the signal without distortion or loss of information. FCC rules require suppression of the signal outside the band to prevent interference.

Cable Fault: Cable faults are damage to cables which affect a resistance in the cable. If allowed to persist, this can lead to a voltage breakdown. There are different types of cable faults, which must first be classified before they can be located.

Cable Landing Station: A facility that houses network equipment facing both the submarine (undersea) and terrestrial (land) networks.

Cellular Technology: This term, often used for all wireless phones regardless of the technology they use, derives from cellular base stations that receive and transmit calls. Both cellular and PCS phones use cellular technology.

CERT: A division of the Software Engineering Institute (SEI), CERT studies and solves problems with widespread cybersecurity implications, research security vulnerabilities in software products, contribute to long-term changes in networked systems, and develop cutting-edge information and training to help improve cybersecurity.

Data 1: A general term for information or a collection of interrelated, unique data items or records, in one or more computer files.

Data-Grade Cable: Cable that is capable of reliably transmitting digital data.

Data Communications: The transmission and reception of data between locations. Data communications require a combination of hardware (terminals, modems, multiplexers, and other hardware) and software.

Data Integrity: The dependability and correctness of data. Vital to organizations and systems that rely upon data to operate, the function supports error detection, correction, and data redundancy.

Encrypt: To alter or encode data to prevent unauthorized access.

European Telecommunications Standard Institute (ETSI): A European standards organization involved with wireless LAN standards.

Fiber-Optic Cable: Thin, transparent fibers of glass or plastic that transmit data through pulses of light from a laser or light emitting diode (LED).

Jam Signal: A signal used to reinforce collisions in a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) LAN so that all transmitting stations are aware of the collision state.

ISAC: Information Sharing and Analysis Centers are non-profit, member driven sector organizations that provide a trusted environment and platform for manufacturers and suppliers to collaborate on cybersecurity and all-hazards threat and mitigation sharing.

Layer: A logically distinct module in the architecture of a network, responsible for particular data communications tasks. It is also called a level.

NAP: Network Access Point.

NITTF: Under joint leadership of the Attorney General and the Director of National Intelligence, the National Insider Threat Task Force (NITTF) works government wide to deter the compromise of classified information by malicious insiders and to establish programs to protect federal classified networks.

NOC: Network Operations Center. Centralized location which monitor security threats to the cable network.

Submarine Communications Cable: Cable laid on the sea bed between land-based stations to carry telecommunication signals across stretches of ocean. Such cables must be specially protected against moisture. At shallow depths on continental shelves, submarine cables commonly are plowed in and armored to protect them against ship anchors, trawler nets, and sharks.

Telecommunications Firm: A type of communications service provider (CSP) (or telecommunications service provider or TSP) that provides telecommunications services such as telephony and data communications access.

OSINT: Open-source intelligence (OSINT) is derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to intelligence requirements.

OTDR: Optical time-domain reflectometer

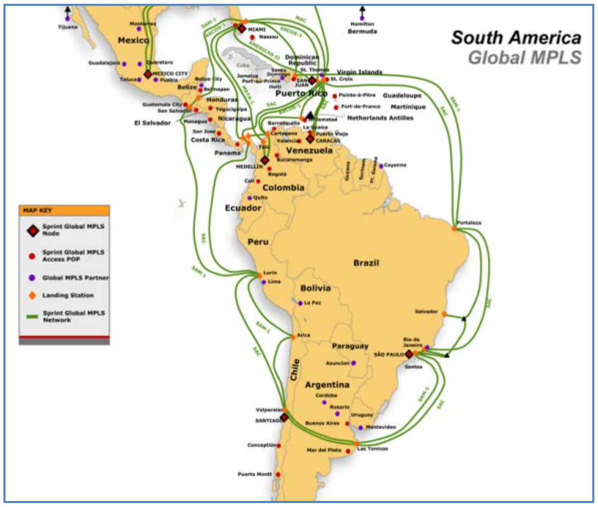
ANNEX II - Submarine Cable Depth Definitions

Depending on the context (nautical navigation, biological, diving, hydrological), multiple lexicons have been used to describe the various depth zones of the sea. For the purposes of this paper, the following definitions have been utilized.

Overland and Last Mile

Many cable systems are designed as a 'virtual' circle for resiliency purposes. In the event of a cable break in one part of the circle, signals can be 'reversed' and transmitted in the opposite direction. Although latency (delays) may increase, and bandwidth capacity may be taxed, the circular design adds a layer of backup transmission. However, a portion of the circular networks often runs overland (e.g. in South America), which exposes the cables and therefore the undersea network traffic to significant disruption by activists, vandalism, and accidents. Cables may also stretch inland out as far as 10 miles from the beach landing point to the first cable landing station, exposing it to similar threats.

South America – Global MPLS[lx]



Near-shore

Near-shore represents the effective depth limit of a recreational diver (~130ft). Recreational licenses and equipment are simple to obtain and require no security background checks. Equipment such as underwater scooters, extending the range of the diver and underwater saws, are easily obtainable and inexpensive. Drug cartels also have their own capable submarines which in 2008 transported an estimated 30% of all drugs imported to the U.S. Some characteristics of the subs include lengths of up to 12-24m, cargo capacity of 2-10 tons, ranges of 3,200 kilometers and depths to 60ft. In 2008 it was estimated that ~80 departures were made from South America. Although Cartels are not considered a direct threat to undersea communications, their ability to rent or sell the subs to adversaries must be considered. Another item to note is that cables are typically buried below the sea-bed 3-6ft out to 20-30ft depths.

Underwater Scooters & Submarines[lxi][lxii]

Off-shore

Off-shore represents the typical limits of a recreational ‘technical’ dive where nitrox tanks allow divers to reach depths of around 300ft. It is also close to the maximum depth of many anchorages for commercial vessels, which are often near cable clusters. Technical licenses and equipment are available for nitrox diving, but are expensive and take extensive time and training to obtain.

Continental shelf

The continental shelf runs from 300 to 600ft. Private, commercial ‘luxury’ submarines can be purchased for these depths, which are design to be launched from private vessels and used for luxury or research purposes, giving access to cables at these depths.

Luxury Submarines & Research Submersible[lxiii][lxiv]

Deep sea

Deep-sea ranges from 600ft to the maximum depths of the ocean. Access to deep sea levels is possible through commercially available ROV subs to as much as 6,000ft. These subs are designed for underwater work and construction and are fitted with remote claws and high intensity lighting. Access to these depths involve state-actor military grade submarines. At these depths cables are usually not buried, but suspended directly on the ocean floor.

Remotely Operated Vehicle (ROV)[lxv]

ANNEX III - Submarine Cable Network History[lxvi]

Early Beginnings

The first transatlantic cable was laid in 1858. Although it only lasted 20 days, it carried 732 messages and saved the British government £50,000. It took sixteen and a half hours to pass a 99 word message from Queen Victoria to President Buchan. The second attempt, in 1866, was more resilient and lasted until the first radio telephone was installed in 1927.

The first submerged repeater was developed by the British Post Office and put into service in 1943. And, the American Telephone and Telegraph Company laid the first deep water repeater in 1950 between Key West and Havana. By 1956, the first transatlantic telephone cable connected Scotland with Newfoundland and shorter distance networks began webbing the ocean and seabeds, connecting countries and facilitating communication speed and frequency. The first transatlantic telephone cable system was a triumph of international cooperation, which brought together governments and private businesses from at least three countries. The final venture included the active participation of the American Telephone and Telegraph Company, the British Post Office and the Canadian Overseas Telecommunications Corporation.

Today, commercial telephone transmissions requiring much greater bandwidth than telegraph occur daily. The greater bandwidth, in turn, requires higher frequencies, which means more attenuation. The technology known as the submerged repeater has enabled the current systems to evolve into the three and four thousand mile undersea systems which exist today.

Designing a Submarine Network

Undersea cable technology requirements also take into account the recommendations and requirements of oceanographers and seamen, and must be laid across ocean beds as free as possible from deep trenches, jagged coral, the corrosive effects of water, and the boring of marine animals. Overall the system must be strong enough to support four or five miles of its own weight in water.

The system has evolved and now consists of combined fiber optic cable with power, branching units, and fiber amplifiers. At the shore end are special terminals for multiplexing signals and supplying power, and fault location equipment. It is a fully complementary system, each part having been built specifically for undersea use.

The first deep water telephone cable was similar to its telegraph counterpart. The only appreciable difference was a concentric return conductor added to form a coaxial structure. The cable had a copper center wire surrounded by three thin copper tapes as its electrical member. A solid dielectric separated the center wire from a helix of six copper tapes. The solid dielectric—made of polyethylene—was necessary because of the high water pressure on the ocean bottom. Around these electrical members were several layers of protective and strengthening materials.

The first undersea cables were laid along existing shipping routes without much concern for the condition of the ocean bottom. Today a sizable amount of preliminary survey work is done to determine the best cable route. Ideally, such a route should avoid deep ocean trenches and steep grades, stay clear of centers of earthquake activity and the rough mountain ranges on the ocean bottom.

During the installation of one of the Pacific Ocean cable systems, oceanographers had to chart vast mountain ranges, deep trenches, thousands of volcanic seamounts and scores of live volcanoes to find an acceptable route for the cable.

Cable Evolution

Telegraph cable did not use copper tapes but usually had strands of copper wire. Both cables were armored by wire rope and were further protected by tar, linseed oil and pitch.

The important difference between the telephone and telegraph systems was the repeater. Telegraph systems had operated for years without them, but telephone systems could not function without periodic boosts from repeaters. In fact the use of different repeaters turned the first transatlantic system into two systems.

Growth and Expansion

Since the first transatlantic system many other systems have been implemented; six span the Atlantic Ocean, while two cross the Pacific. Currently under construction is a system which will link Cape Town, South Africa and Lisbon, Portugal.

The system used in the deep water section of the first transatlantic cable—dubbed the SB cable system—has been altered and been progressively supplanted. Originally the SB system had thirty- six 4-kHz voice channels. To optimize the use of these channels TASI (Time Assignment Speech Interpolation) was applied. TASI enabled the ability to switch unused speech channels to a talker within milliseconds and switch away again to another user when the first talker stopped to listen. In effect TASI doubled the number of speech channels available.

In 1959 a new modulation scheme, called double modulation, was introduced to the SB system which reduced the 4-kHz voice channel to a 3-kHz channel. When double modulation was introduced it was possible to obtain 48 voice channels in the same frequency range that had initially only carried 36.

Satellite Technology vs. Undersea Cables

Although satellite technology does rival that of undersea cable growth, undersea systems do not require the large, expensive terminals satellite systems do. In fact their fixed terminal points make undersea systems ideal for daily, well established international telephone service. Furthermore, the ocean floor does not limit the number of undersea cables as much as the available area for synchronous satellite orbits.

However, satellites are more flexible and resilient than undersea systems as they usually carry several repeaters, thereby avoiding complete system failures caused by the loss of a single repeater. Terminal points in a satellite system can also be changed, making it possible to re-route traffic when necessary.

ANNEX IV - Additional Resources

The following resources do not constitute an exhaustive list but rather a sample of government and public-private membership organizations relevant to the submarine cable industry, which provide education, resources, events, and partner networks.

Atlantic Cable Maintenance & Repair Agreement (ACMA)

ACMA is a non-profit cooperative subsea maintenance agreement consisting of 59 members. ACMA embers are companies responsible for the operations and maintenance of undersea communications and power cables, as well as Oil & Gas Platform operators, in the Atlantic, North Sea and Southeastern Pacific Ocean.

Contact Info:
CTO
Deep Blue Cable
Phone: +1 758 730 5555
http://www.acma2017.com/

Carnegie Mellon University - CERT

The Department of Homeland Security (DHS) and the CERT Division mutually set goals in areas such as data collection and mining, statistics and trend analysis, computer and network security, incident management, insider threat, software assurance, and more. The results of this work include exercises, courses, and systems that were designed, implemented, and delivered to DHS and its customers as part of the SEI's mission to transition SEI capabilities to the public and private sectors and improve the practice of cybersecurity.

Contact Info:
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
+1 412-268-5800
http://www.cert.org/

The Communications Security Reliability, and Interoperability Council (CSRIC)

The mission of the Communications Security, Reliability and Interoperability Council (CSRIC) is to provide recommendations to the Federal Communications Commission (FCC) to ensure optimal security and reliability of communications systems, including telecommunications, media, and public safety. The CSRIC has identified best practices and developed recommendations to identify, protect, detect, respond to, and recover from cyber events.

Contact Info:
Federal Communications Commission
445 12th Street SW
Washington, DC 20554
+1 888-225-5322
https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0

The International Cable Protection Committee (ICPC)

IPC has been representing the undersea cable industry since it was founded in 1958 with the vision to be the premier international submarine cable authority, providing leadership and guidance on issues related to submarine cable security and reliability. The ICPC provides a forum in which relevant technical, legal and environmental information is exchanged among its international members.

Contact Info:
International Cable Protection Committee
PO Box 150
Lymington SO41 6WA
United Kingdom
+44 7836 249376
https://www.iscpc.org/

IEEE

IEEE, pronounced "Eye-triple-E," stands for the Institute of Electrical and Electronics Engineers. The association is chartered under this name and it is the full legal name. IEEE and its members inspire a global community to innovate for a better tomorrow through its more than 420,000 members in over 160 countries, and its highly cited publications, conferences, technology standards, and professional and educational activities.

IEEE is the trusted “voice” for engineering, computing, and technology information around the globe.

Contact Info:

Society information
Phone: +1 732 562 5501
Email: society-info@ieee.org
IEEE Member and Geographic

Activities
Phone: +1 732 562 5501
Fax: +1 732 463 9359
Email: mga@ieee.org

Technical Activities
Phone: +1 732 562 5501
Email: contactcenter@ieee.org

Section and Chapter Information
Phone: +1 732 562 5511
Fax: +1 732 463 9359
Email: sec-chap-support@ieee.org

The North American Submarine Cable Association (NASCA)

The North American Submarine Cable Association, or NASCA, is a non-profit organization of companies that own, install or maintain submarine telecommunications cables in the waters of North America. NASCA serves as a forum for its membership to provide and exchange information on technical, legal, and policy issues of common interest. These issues include standards and procedures for government approval of new cable installations; working relationships with other marine industries; and public education about such cables. NASCA was formed in October 2000. NASCA is seeking IRS recognition as a non-profit trade association and business league under section 501(c)(6) of the Internal Revenue Code.

Contact Info:
secretariat@n-a-s-c-a.org

National Telecommunications and Information Administration (NTIA)

The National Telecommunications and Information Administration (NTIA), located within the Department of Commerce, is the Executive Branch agency that is principally responsible by law for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the internet remains an engine for continued innovation and economic growth. These goals are critical to America's competitiveness in the 21st century global economy and to addressing many of the nation's most pressing needs, such as improving education, health care, and public safety.

Contact Info:
https://www.ntia.doc.gov/home

TeleGeography
TeleGeography is a telecommunications market research and consulting firm, which conducts in-depth research, compiles large data sets, and presents this information clearly in online reports and databases to support clients, including service providers, equipment makers, investors, and governments.

Contact Info:
www.telegeography.com

References

[i] Website; Fiber Transceiver Solution; “Essay About Submarine Cable Systems”; http://www.fiber-optic-transceiver-module.com/essay-about-submarine-cables-system.html; accessed 7 August 2017. Online news article from a telecommunications firm.

[ii] Website; “TeleGeography Submarine Cable Map”; https://www.submarinecablemap.com/; Accessed August 8, 2017.

[iii] Website; Techradar.pro; “The Incredible Story of the Underwater Internet”; http://www.techradar.com/news/Internet/the-incredible-story-of-the-underwater-Internet-1291295; Accessed August 7, 2017; Online news article from TechRadar, an international media group.

[iv] Website; Unclos Debate; https://www.unclosdebate.org/argument/861/underseas-cables-are-vital-global-economy

[v] Website; TeleGlobe; http://www.visualcomplexity.com/vc/project.cfm?id=160

[vi] Website; Science Friday Initiative Inc,; https://www.sciencefriday.com/articles/the-undersea-network-that-connects-the-world/

[vii] Co-chairs Report on the Safety and Security of Vital Undersea Communications Infrastructure, Council for Security Cooperation in the Asia Pacific (CSCAP), February 2014.

[viii] Submarine Telecoms Forum 94, May 2017, p. 28.

[ix] 5th Annual Submarine Telecoms Industry Report, Issue 5, Oct 2016.

[x] Website; TE Subcom; https://www.youtube.com/watch?v=Gsoo_BOwrrM

[xi] Website; Light Wave Online; http://www.lightwaveonline.com/articles/2017/02/xtera-emerges-from-bankruptcy-with-new-ownership.html

[xii] 5th Annual Submarine Telecoms Industry Report, Issue 5, Oct 2016 p 14.

[xiii] Submarine Cable Almanac, issue 22, copyright May 2017, Submarine Telecoms Forum.

[xiv] Website; Egypt Independent; http://www.egyptindependent.com/Internet-saboteur-caught-says-telecom-egypt-ceo/

[xv] “Submarine Cables, Security, and the State” by John Tibbles; Submarine Telecoms Forum 94, May 2017.

[xvi] Website; Research Gate; https://www.researchgate.net/publication/224468601_Understanding_Danger_to_Critical_Telecom_Infrastructure_A_Risky_Business

[xvii] Website; Research Gate; https://www.researchgate.net/publication/224468601_Understanding_Danger_to_Critical_Telecom_Infrastructure_A_Risky_Business

[xviii] 5th Annual Submarine Telecoms Industry Report, Issue 5, Oct 2016 pp 14-17.

[xix] New Threats, Old Technology: Vulnerabilities in undersea communications cable network management systems, February 2012, Michael Sechrist.

[xx] Website; The Sydney Morning Herald; http://www.smh.com.au/federal-politics/political-news/australia-refuses-to-connect-to-undersea-cable-built-by-chinese-company-20170726-gxj9bf.html

[xxi] CSRIC IV Working Group 8 Report, Dec 2014, p. 10.

[xxii] Co-chairs Report on the Safety and Security of Vital Undersea Communications Infrastructure, Council for Security Cooperation in the Asia Pacific (CSCAP), February 2014.

[xxiii] AEP Phone interview, Service Provider manager, August 2, 2017.

[xxiv] Michael Sechrist, personal interview, August 2nd, 2017.

[xxv] Website; BT Group; https://www.btplc.com/civilresilience/Casestudies/UKResponse/KyleOfLochalsh.html

[xxvi] Website; Panoramio; http://mw2.google.com/mw-panoramio/photos/medium/95243150.jpg

[xxvii] Website; Gate Marine; http://www.gatemarine.com/en/pages/services/submarine-cable/

[xxviii] Website; BBC Image via Modern Survival Blog; http://modernsurvivalblog.com/natural-disasters/freak-uk-mini-tsunami-a-reminder-of-puerto-rico-trench-hazard/

[xxix] Captain Douglas R. Burnett, U.S. Navy (Retired). (2011). *Cable Vision*. Pg. 69

[xxx] Website; The New Economy; https://www.theneweconomy.com/insight/the-sharks-that-are-biting-into-googles-cable-systems
[xxxi] Website; Alaska Communications; http://akorn.alaskacommunications.com/_/img/IMG-fiberopticcables.png; Accessed August 18, 2017.
[xxxii] Council for Security Cooperation in the Asia Pacific. (25 February 2014). *Co-Chair's Report on the Safety and Security of Vital Undersea Communications Infrastructure*. Pg. 3
[xxxiii] Website; Josh Ruppe, Security Researcher, Speaker, & Penetration Tester; https://www.joshruppe.com/fiber-optics-introduction/
[xxxiv] Council for Security Cooperation in the Asia Pacific. (25 February 2014). *Co-Chair's Report on the Safety and Security of Vital Undersea Communications Infrastructure*. Pg. 3
[xxxv] Captain Douglas R. Burnett, U.S. Navy (Retired). (2011). *Cable Vision*. Pg. 6
[xxxvi] Website; Digital Guardian; https://digitalguardian.com/blog/what-insider-threat-insider-threat-definition
[xxxvii] Web site; CERT; http://www.cert.org/insider-threat/; Accessed on August 18, 2017.
[xxxviii] Website; Carnegie Mellon University; http://www.cert.org/insider-threat/cert-insider-threat-center.cfm
[xxxix] National Security Telecommunications Advisory Committee. (2007). Report to the President on International Communications.
[xl] United Nations Environment Programme-World Conservation Monitoring Centre. (2009). Submarine Cables and the Oceans: Connecting the world. Retrieved from https://www.iscpc.org/publications/
[xli] Davenport, Tara. (2015). Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. Catholic University Journal of Law and Technology
[xlii] Department of Homeland Security. National Protection and Programs Directorate. Office of Infrastructure Protection. Integrated Analysis Task Force. National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat (2013). Retrieved from https://scadahacker.com/library/Documents/Insider_Threats/DHS%20-%20Risks%20to%20US%20Critical%20Infrastructure%20from%20Insider%20Threat%20-%2023%20Dec%2013.pdf
[xliii] Rauscher, Karl Frederick. The Reliability of Global Undersea Cable Community Infrastructure Report. (2010). IEEE Communications Society. Retrieved from https://scadahacker.com/library/Documents/Insider_Threats/DHS%20-%20Risks%20to%20US%20Critical%20Infrastructure%20from%20Insider%20Threat%20-%2023%20Dec%2013.pdf
[xliv] Rauscher, Karl Frederick. The Reliability of Global Undersea Cable Community Infrastructure Report. (2010). IEEE Communications Society. Retrieved from https://scadahacker.com/library/Documents/Insider_Threats/DHS%20-%20Risks%20to%20US%20Critical%20Infrastructure%20from%20Insider%20Threat%20-%2023%20Dec%2013.pdf
[xlv] ROGUCCI Global Summit Report; http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf
[xlvi] Department of Homeland Security, op. cit.
[xlvii] SCADA lecture http://nptel.ac.in/courses/108106022/LECTURE%208.pdf
[xlviii] Luallen, Matthew E. Managing Insiders in Utility Control Environments. (2011). SANS Institute.
[xlix] Sechrist, Michael. New Threats Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems. (2012) Retrieved from http://www.belfercenter.org/sites/default/files/files/publication/sechrist-dp-2012-03-march-5-2012-final.pdf
[l] Davenport, Tara. (2015). Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. Catholic University Journal of Law and Technology.
[li] Department of Homeland Security. National Protection and Programs Directorate. Office of Infrastructure Protection. Integrated Analysis Task Force. National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat (2013). Retrieved from https://scadahacker.com/library/Documents/Insider_Threats/DHS%20-%20Risks%20to%20US%20Critical%20Infrastructure%20from%20Insider%20Threat%20-%2023%20Dec%2013.pdf
[lii] Rauscher, Karl Frederick. The Reliability of Global Undersea Cable Community Infrastructure Report. (2010). IEEE Communications Society. Retrieved from https://scadahacker.com/library/Documents/Insider_Threats/DHS%20-%20Risks%20to%20US%20Critical%20Infrastructure%20from%20Insider%20Threat%20-%2023%20Dec%2013.pdf

[liv] Website; Subsea World News; http://www.ecmag.com/section/your-business/supply-submarine-cable-face-significant-strain

[lv] Website; AOL; https://www.aol.com/2012/12/21/more-than-1100-new-submarine-electricity-cable-sys/

[lvi] Website; CERT; http://www.cert.org/insider-threat/

[lvii] Website; NIST, https://www.nist.gov

[lviii] National Insider Threat Task Force (NITTF), "Protect Your Organization from the Inside Out: Government Best Practices" 2016

[lix] U.S. Dept of Justice Federal Bureau of Investigation, "The Insider Threat" brochure – An introduction to detecting and deterring an insider spy

[lx] Website; Sprint; https://www.sprint.net/images/South-America-GMPLS.png.

[lxi] Website; Adventure Junkies; https://www.theadventurejunkies.com/best-underwater-scooter/; Accessed August 18, 2017.

[lxii] Website; Motherboard; https://motherboard.vice.com/en_us/article/vvbwwb/the-hunt-for-narco-subs; Accessed August 18, 2017.

[lxiii] Website; Super Yachts; http://www.superyachts.com/syv2/newsimages/584/290/90/c/3e74/cms/luxury_style/11983-from-sky-to-water-luxury-submarine-to-feature-private-jet-interior-.jpg; Accessed August 18, 2017.

[lxiv] Website; MarineLink; https://www.marinelink.com/news/development-submersible360822; Accessed August 18, 2017.

[lxv] Website; Investment Casting Space Shuttles; https://i.pinimg.com/736x/f0/36/8c/f0368c4a8627a5ca64053d49e5d68209--investment-casting-space-shuttles.jpg; Accessed August 18, 2017.

[lxvi] Website; Atlantic Cable; http://atlantic-cable.com/Article/1968Lenkurt/index.htm

2017
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA

NCTC 031991 ID 9-17