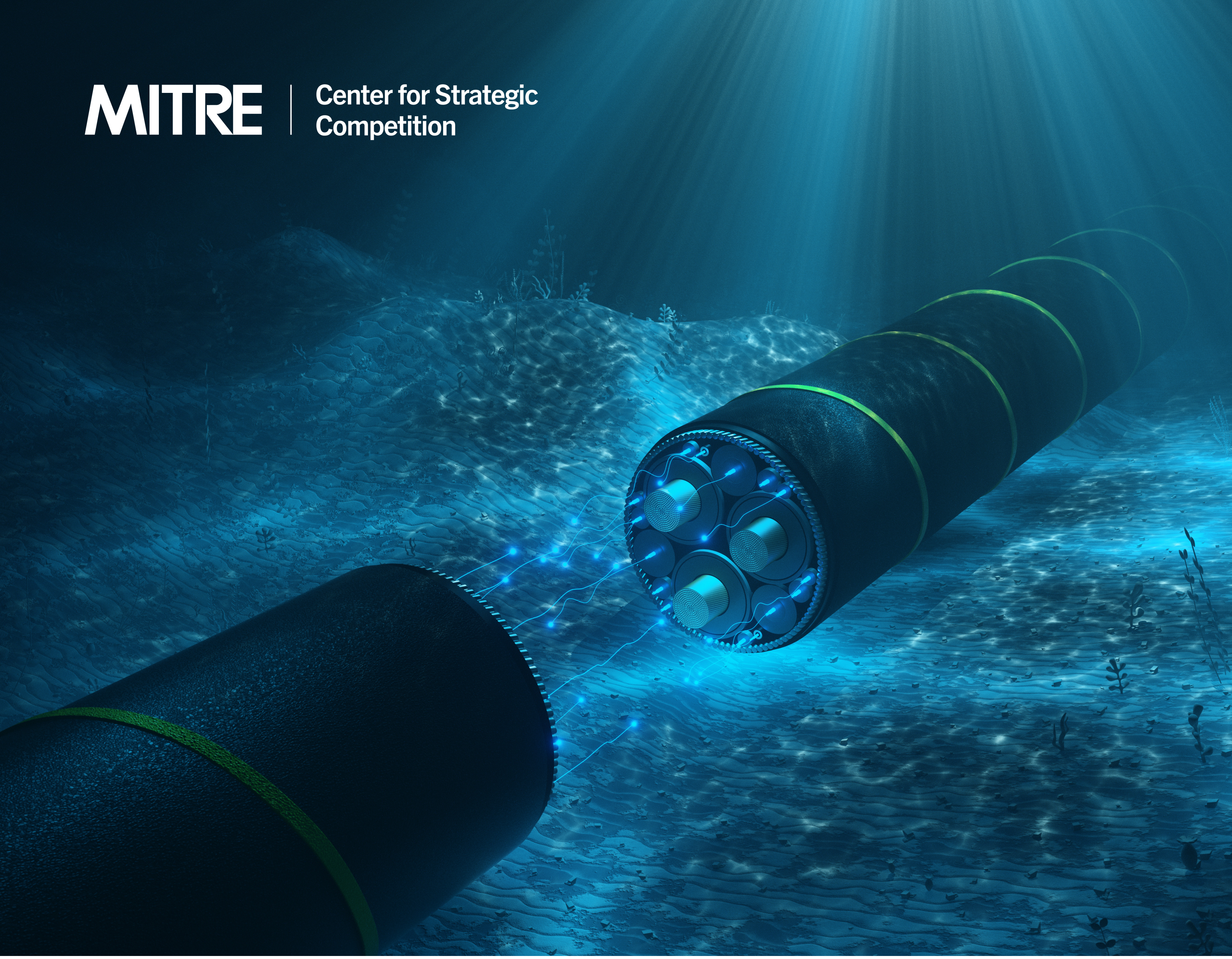
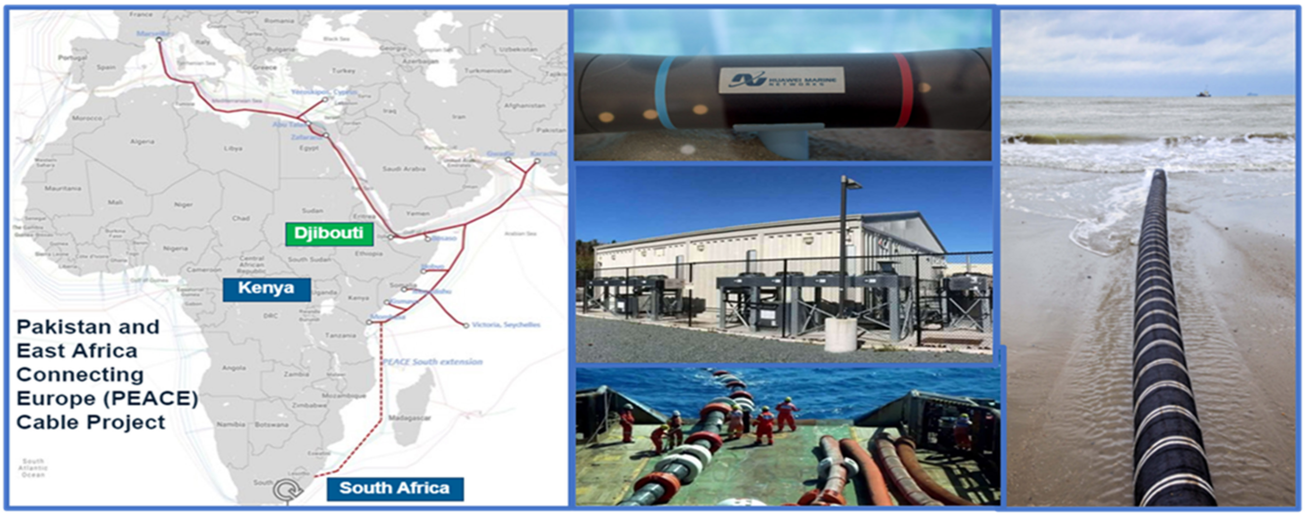
MITRE | Center for Strategic Competition



DIGITAL SILK ROAD PEACE SUBSEA CABLE CONNECTIONS TO THE ICT

Nancy Ross and Maggie Vencill



Subsea cables, much like other information and communications technology components, are often taken for granted. Of particular interest to the study of the Digital Silk Road (DSR) are the subsea cables and cable landing stations that advance the People's Republic of China's (PRC) strategy for global digital dominance.

This paper is an update to "Undersea Cable Connections to the ICT, Digital Silk Road PEACE" first written in 2021 and released for unlimited distribution under MITRE's public release case number 21-2737. The primary changes include an update to the cable landing station (CLS) technology, and the addition of recent subsea cable disruption examples and emerging subsea cable system vulnerabilities.

The Role of Subsea Cables

Subsea (also referred to as undersea) cables are a key part of the world's information superhighways, used to make over 10 trillion U.S. dollars (USD) of financial transactions each day and carry an estimated 95 to 99 percent of the world's voice and electronic data traffic.[1,2] As the world continues to digitize, many more cables will be needed. Over the next few years, the number is expected to grow by some 30 percent annually.[3] The subsea cables connect to terrestrial cables and move data between a wide variety of end users and services via data centers, the cloud, and internet exchange points (IXPs). Many of the newest and longest routes are being financed, designed, and built by hyperscalers like Amazon, Google, Meta, and Microsoft.

The Pakistan & East Africa Connecting Europe (PEACE) submarine cable system, connecting Asia, Africa, and Europe, provides open, flexible, and carrier-neutral services to its customers.[4] PEACE, as part of the DSR, is a high-speed, 15,000-kilometer undersea cable system that, when complete, will offer high-capacity, low-latency routes connecting China, Europe, and Africa.[5]

PRC'S EMERGENCE AS A LEADING PROVIDER OF UNDERSEA CABLES REQUIRES ATTENTION. EMPLOYING ZERO-TRUST TECHNOLOGIES AND GREATER DATA SECURITY COUPLED WITH THE USE OF ALTERNATIVE CABLE ROUTES WILL REDUCE RISK OF SENSITIVE DATA COMPROMISE OVER HIGH-RISK CABLE ROUTES.

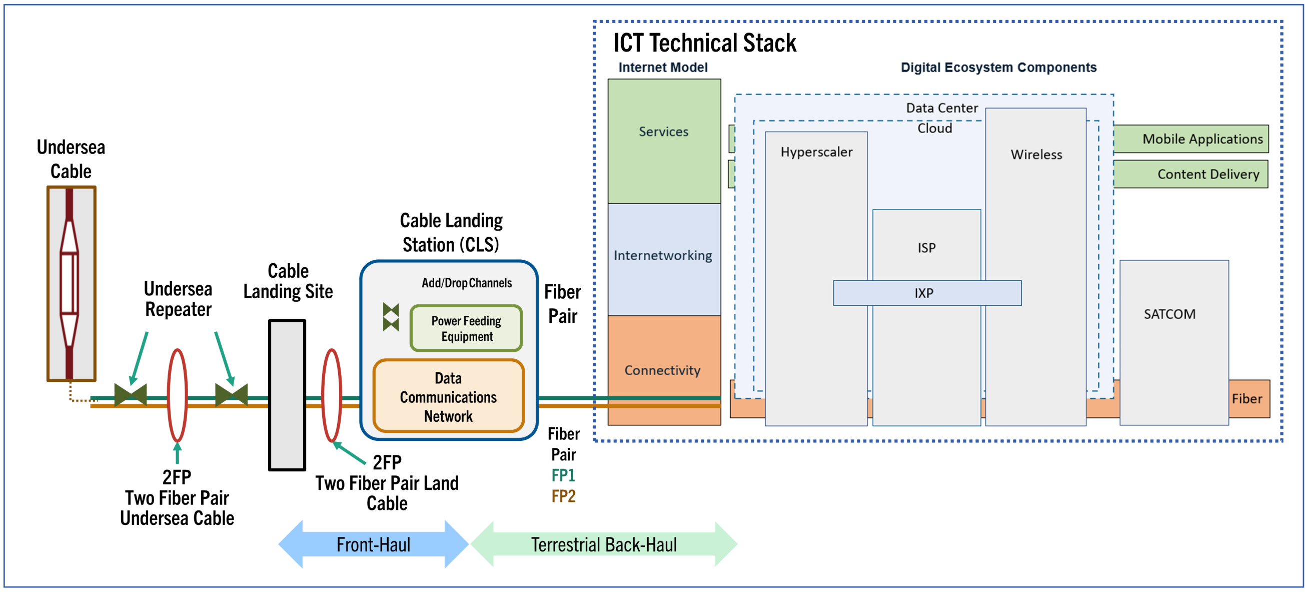
PEACE also has the potential to yield economic benefit for eastern African states. MITRE's DSR economic impact study indicates that Djibouti's PEACE cable could raise gross domestic product (GDP) by as much as $7 million, or 0.19 percent, in year one due to its unique geographical position. The average annual GDP would increase $4 million, or 0.04 percent, in each of years two through five.[6]

An understanding of the vulnerabilities of subsea cable systems and their connection to the information and communications technology (ICT) stack (e.g., data centers) highlights the need to apply zero-trust principles and identify innovative resiliency solutions. Zero-trust oriented technologies will assist with ensuring network management system updates and improving data security. Examples of zero-trust technology firms could not be identified for the CLS locations covered in this paper. However, CMC Networks, based in Johannesburg, South Africa, offers security solutions across networks and subsea cable systems in many DSR locations. In addition, use of private and third-party cable routes will also reduce the risk of sensitive data compromise over high-risk cable routes.

Key Components of Subsea Cables

1. **Subsea cables**
2. **Cable landing sites**
3. **Cable landing stations**

As subsea cables surface from the ocean floor toward terrestrial infrastructure, they traverse the beach to a cable landing site. Once they reach land, the cables (aka front-haul cables) connect to a CLS, where the optical signals convert to electrical signals before being sent via terrestrial fiber back-haul connections to the data center. At this point, the subsea cable system is connected to the ICT stack. Data from subsea cables can be routed via IXPs or OTT (Over The Top) service providers to other locations or be directed to local provider services hosted within that data center.



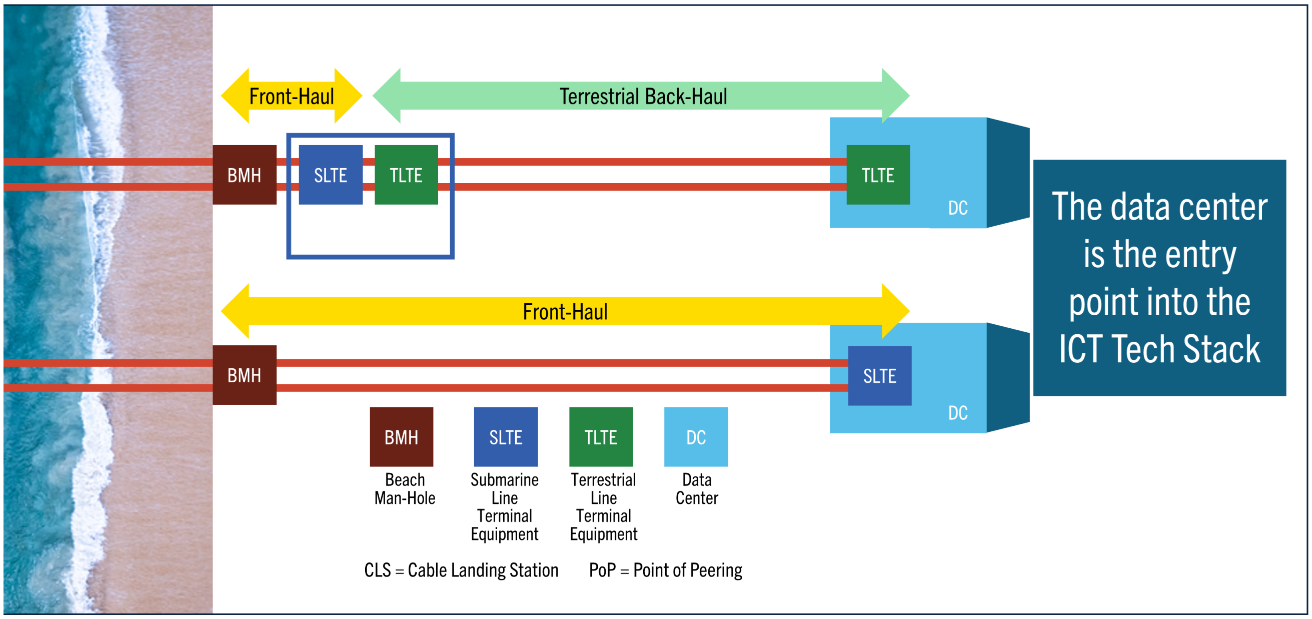
Three Models

Two of the primary CLS deployment models, depicted below, have been identified along the DSR.

The first is a more conventional model, where the CLS is located between the cable landing site and the data center. Typically, there is considerable distance between the landing site and the data center. Terrestrial Line Terminal Equipment (TLTE), located in the CLS, connects the CLS to the data center. Djibouti CLSs are an example of this model.

The second model is a City Point of Presence (PoP) model, in which the CLS is colocated within the data center near the coastline.[7] This model is deployed in locations where cities can leverage the proximity of modern data centers with that of cable landing sites. The primary difference between the conventional model and the City PoP model is that there is no terrestrial back-haul cable present, only front-haul cable to the Submarine Line Terminal Equipment (SLTE), which allows the CLS to be colocated directly inside the data center. A DSR example of this model is the original MRS2 CLS in Marseille, France. The City PoP eliminates several vulnerability points in the subsea cable system, although it does add some complexity in the data center.

The third model emerging is the CLS Campus model. The City PoP model has been evolving over the past few years into what industry leaders refer to as CLS Campuses or Hubs. MRS2 in Marseille is an excellent example of a City PoP model that has evolved into a state-of-the-art CLS Campus. The evolution has been spurred on because the CLS can no longer be a passive interconnection point to a faraway hub for carriers. The genesis of this new concept comes from OTT provided services like internet streaming platforms. OTT services bypass traditional platforms to deliver content directly to


Front-Haul
Terrestrial Back-Haul
BMH
SLTE
TLTE
TLTE
DC
Front-Haul
BMH
SLTE
DC
The data center is the entry point into the ICT Tech Stack
BMH Beach Man-Hole
SLTE Submarine Line Terminal Equipment
TLTE Terrestrial Line Terminal Equipment
DC Data Center
CLS = Cable Landing Station
PoP = Point of Peering

Conventional CLS vs. City PoP

users online. Global connectivity, driven by OTTs, requires multiple terrestrial options to connect to the CLS and then multiple subsea networks to route across oceans with diverse landings in the next continent creating a CLS hub.[8]

Vulnerabilities

Subsea cables have physical and digital vulnerabilities. Roughly 75 percent of all reported incidents are accidental.[9] However, recent cable outages have created real concern and speculation about whether there is a trend of subsea cables being intentionally cut. In early February 2024, Yemen's internationally recognized government in exile alleged that the Houthis planned to attack undersea cables.[10] On February 24, 2024, SEACOM cables appear to have been cut, causing SEACOM, which serves Djibouti, to suffer interruptions. The disruption ran from Mombasa, Kenya, to Zafarana, Egypt. On March 4, 2024, three cables under the Red Sea that provide global internet and telecommunications were damaged as a result of a Houthi attack on a cargo ship in the Red Sea. Several undersea cables off the coast of Yemen in the Red Sea, carrying huge amounts of data and communications, suddenly went dark on March 14, 2024. The outage affecting 13 African countries including South Africa caused loss of internet connectivity and disruptions to mission-critical cloud and data center services. Preliminary analysis points to seismic activity in the area rather than human activity. Estimates are that repairing the damaged undersea cables will take months and require re-routing of traffic through other cables.

While physical damage, whether intentional or not, to undersea cables accounts for the majority of reported undersea cable outages, a variety of vulnerabilities exist at nearly every point along the subsea cable system, including:

- Protection of CLS ownership interests may prompt the need for military presence in the vicinity of landing sites and CLSs.
- Maintenance or research vessels have the potential to mask covert operations.
- Increased use of advanced technologies that enable remote monitoring systems may inadvertently expose cables and ICTs, through which the systems are connected, to hacking risks.
- Regional conflicts and military operations pose threats to subsea cables and downstream consequences to ICT operations.
- Subsea cables are a target for cyber threats including espionage and attack capabilities.[11, 12]
- Disabling undersea repeaters could interrupt data flow.
- Cables at landing sites and fiber pair termination points as well as adjacent terrestrial back-haul cables could be damaged/severed.
- Physical breaches to a CLS such as cutting off power supply could pose a target for those intending to interrupt the flow of critical, sensitive data.

The security of subsea cables, the CLS, and the connection to the ICT stack is of growing concern. During a cable system's 25-year life cycle, inevitable geopolitical changes cause fluctuations in trust between governments. PRC's emergence as a leading provider of undersea cables could make industrial espionage alluring[13] and highlights the need for increased digital security.

Improved monitoring and maintenance of existing subsea cables using advanced sensors and technologies are helping detect anomalies in data flows or cable breaches and allow cable operators to avoid (or minimize) outages. Two examples of advanced technologies being developed are artificial intelligence–powered monitoring systems to predict data outages and cable failures and robotic systems such as underwater autonomous vehicles/remotely operated vehicles (AUVs/ROVs) to inspect, maintain, and repair cables. Advanced encryption, intrusion detection, and zero-trust approaches will enable greater security for data traversing undersea cable systems. Employing zero-trust architecture and principles focuses on evaluating trust related to data security on a per-transaction (and associated user or user device) basis, which can protect against common threats to data security.[14]

The protection of undersea cable systems will benefit from collaborative international initiatives and global partnerships to promote cooperation among nations, industries, and academic institutions. Global partnerships will help promote research aimed at protecting underwater infrastructure. Creating global alliances will also protect undersea cable systems and thwart the ability of authoritarian-controlled or state-owned companies to intercept data and create technology dependencies through regions impacted by the DSR.

In addition, the ability to effectively evaluate the riskiness of sharing sensitive data over PEACE cables, as opposed to other cable routes available in DSR areas, requires the development of risk criteria and risk models. A risk assessment model would also assist in identifying potential data security breaches and mitigations.

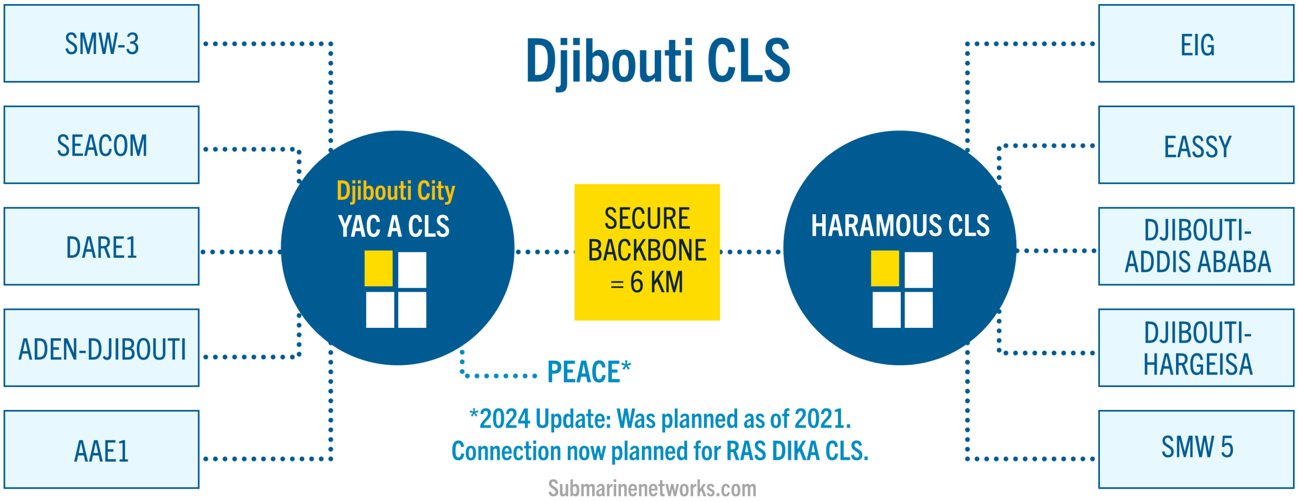
The following PEACE cable sites are examples of CLS models, and highlight risks related to PRC influence.

Djibouti CLSs

Djibouti is a significant location for subsea cables running through the PEACE corridor and is an example of a conventional CLS connection to the data center/ICT. Djibouti Telecom is the incumbent telecommunications monopoly in Djibouti. In addition to PEACE, the PRC has established a naval presence in Djibouti.

Djibouti Telecom operates two cable landing stations: the Djibouti City (or YAC A) CLS and the Haramous CLS.

According to the Submarinenetworks.com[15] website, there are a total of eight submarine cables and two terrestrial cables creating a strategically positioned international hub connecting Djibouti to telecommunication services in East Africa.



*2024 Update: Was planned as of 2021. Connection now planned for RAS DIKA CLS.

Submarinenetworks.com

According to Infrapedia maps, Djibouti City CLS also includes a PEACE cable.[16] As of the close of 2021, Djibouti Telecom had not yet reported PEACE as landing in the YAC A CLS; however, plans to host PEACE in Djibouti were confirmed.[17] The Haramous CLS links Djibouti with Somalia via the Djibouti-Hargeisa terrestrial cable and with Ethiopia via the Djibouti Addis Ababa terrestrial cable.

In addition to the two CLSs, the Djibouti Data Center (DDC), which is also operated by Djibouti Telecom, is a key carrier-neutral data center in Djibouti. The DDC is located adjacent to the Haramous CLS and is directly connected to both the Haramous CLS and the Djibouti City CLS.

RAS DIKA CLS

Djibouti Telecom's third, and newest, cable landing station in Djibouti City, the RAS DIKA CLS, became operational in August 2023 and is billed as a neutral digital port. The RAS DIKA CLS plans to host six new subsea cable systems: PEACE, 2Africa, Africa-1, SMW6, India-Europe-Express (IEX), and Google's Blue-Raman. IEX, an India-centric subsea cable system, is owned by Jio, which is at the forefront of India's explosive growth in digital services and data consumption, including the demands of streaming video, remote workforce, 5G, and Internet of Things (IoT). The IEX landing completed in late 2023 connects Mumbai to Europe and interconnects with the India-Asia-Xpress in Mumbai, extending its reach to Singapore. The SEA-ME-WE 6 (SMW6) and Africa-1 submarine cables are due to be completed in 2024. These additions will greatly expand Djibouti's submarine cable network and international connectivity. Blue-Raman will also be hosted at the RAS DIKA CLS. According to All Israel News, the Blue Submarine Cable System will connect Italy, France, Greece, and Israel, and the Raman Submarine Cable System will connect Jordan, Saudi Arabia, Djibouti, Oman, and India, bypassing terrestrial cables across Egypt.[18] The RAS DIKA CLS will effectively solidify Djibouti's access to subsea cable systems, transforming Djibouti into an international ICT hub.

Mombasa, Kenya, CLS

PEACE Cable International Network Co. has announced the deployment of a submarine cable system at iColo's data center in Mombasa, Kenya. The data center, known as MBA2, is situated in Nyali in the northern part of the city, was completed in the first quarter of 2022, and is strategically located approximately 2 km from subsea cable landing points (e.g., beach manhole according to the MBA2 technical specifications), making it ideal for reliable colocation services in the region. Multiple local and international telecom carriers colocated in MBA2 ensure reliable, redundant connections.[19] While state-of-the-art, the MBA2 is another example of a conventional CLS connection to the data center/ICT. The investment in submarine cables is of strategic importance to Telkom, Kenya's leading telecommunications service provider, where access to the ICT is growing due to the sharp increase in the demand for internet services, including cloud computing, streaming, gaming, connected devices, and seamless service provision with no interruption. This ultra-high capacity PEACE cable will assist Kenya and the region in meeting current and future broadband capacity requirements and bolster redundancy, minimizing transit time of Kenya's connectivity to Asia and Europe.

PEACE's landing makes it the sixth submarine cable landing in Kenya, preceded by Djibouti Africa Regional Express 1, SEACOM, East African Marine System, Eastern African Submarine Cable System, and Lion2 submarine cable systems.

South Africa CLSs

South Africa is strategically situated for connecting to several subsea cable routes including PEACE (also referred to as PEACE South). PEACE's second phase involves extending the cable to southern Africa, boosting bandwidth and connectivity from its current African landing point in Mombasa, Kenya, all the way to South Africa, and opening new markets to cable partners in the Southern African Development Community and East Africa.[20]

The South African CLSs appear to be examples of a conventional CLS model, where CLSs are separate from the data centers, in part due to distance.

There are two cable landing stations: Mtunzini CLS and Amanzimtoni CLS on the east coast of South Africa. PEACE was projected to land on the east coast of Africa in 2021; however, completion is unconfirmed. IOX Cable System, another new cable system, was also projected to land on the east coast of South Africa in 2022 or later. Telkom South Africa owns and operates the Mtunzini CLS to support the South African Far East (SAFE), SEACOM, and Eastern Africa Submarine Cable System cable landings. Liquid Telkom (formerly Neotel) also operates in the Mtunzini CLS to support SEACOM. Liquid Telkom owns and operates the Amanzimtoti CLS supporting the Melting Pot Indianoceanic Submarine System cable landing with a back-haul connection to the Teraco data center.

There are also two CLSs (Melkbosstrand CLS and Yzerfontein CLS) on the west coast of South Africa. The Melkbosstrand CLS is currently operated by Telkom for the South Atlantic-3/West Africa Submarine Cable and SAFE cable landings, with Google's Equiano cable landing under construction. Telkom also operates the Yzerfontein CLS for the West African Cable System cable landing.

> “THE PEACE SOUTH EXTENSION WILL HAVE AN IMPORTANT IMPACT ON CONNECTIVITY FROM ITS CURRENT AFRICAN LANDING POINT IN MOMBASA ALL THE WAY TO SOUTH AFRICA, OPENING NEW SOUTHERN AFRICAN DEVELOPMENT COMMUNITY (SADC) AND EAST AFRICAN MARKETS TO CABLE PARTNERS.”
>
> Winston Qui, PEACE,
> February 2020, submarinenetworks.com[25]

Marseille, France, CLSs

The Marseille cable landing stations and data center are an example of the CLS Campus model described earlier.[21] While there are multiple data centers colocated in former naval facilities near the coastline in Marseille, the focus is on Interxion's MRS2 data center that boasts content delivery to 4.5 billion people.[22] Interxion operates the MRS2 data center, which provides a total of 13 undersea cable connections to Africa, the Middle East, and Asia. The PEACE-MED cable, which is the trunk of the PEACE subsea cable project, lands in MRS2. PEACE-MED enhances the competitiveness of Marseille Network Hubs while contributing to the expansion of the PEACE market and provides the shortest and most direct data route from Asia to Europe combined with exceptionally low latency, which is vital for connecting through the innovative use of ICT.[23]

The MRS2 CLS also affords PEACE the potential for access to European IXPs, more than 130 connectivity providers, multiple cloud providers, and more than 45 data centers across Europe. Of particular interest to the PRC, according to PEACE's news network, is the ability for the PEACE cable to extend its system's reach to additional markets, such as Frankfurt and Paris.[24]

> “SELECTING THE RIGHT DATA CENTER IN EUROPE FOR THE PEACE [UNDERSEA] CABLE TO INTERCONNECT WITH IS A CRITICAL COMPONENT TO ENSURE THE PROJECT’S COMMERCIAL SUCCESS. WE KNOW THAT WITH INTERXION WE HAVE MADE THE RIGHT STRATEGIC DECISION.”
>
> Sun Xiaohua, Chief Operating Officer of the PEACE Cable International Network Co. Ltd.[26]

These PEACE examples highlight the potential to control a vast amount of data, whether through direct or indirect connections to the ICT stack.

Key Observations on DSR Subsea Cables

DSR subsea cables and their security are of critical importance to eastern Africa. Several key observations to consider are as follows:

- Strategic connections exist between PEACE and several eastern Africa data centers.
- Evidence of a correlation between subsea cable system ownership and military presence exists in Djibouti.
- Increases in the used (e.g., consumed) international bandwidth caused by PEACE are expected to expand communications and create economic growth.
- Multiple vulnerabilities exist along subsea cable routes, creating targets for physical and cyber threats.
- Physical and logical security breaches have the potential to intercept or interrupt data flow.

Subsea cable projects that exponentially increase used international bandwidth in the eastern African region are expected to contribute to economic growth. U.S. policy aimed at developing this region should consider supporting such projects. MITRE research found that subsea cables making new bilateral connections and deepening connections within a region may be most likely to create such growth. The recent subsea cable outages highlight the adverse impact to entire populations and regions with loss of cable availability.

U.S. and other military interests in eastern Africa need to consider the potential risk posed by the PRC’s ability to collect, mine, and use data flowing through the PEACE cables. Recent growing political unrest in the Red Sea region, although linked to other political actors, clearly demonstrates the impact the PRC could have on eastern Africa as well as global connections via the DSR.

For instance, leveraging private or third-party branches from non-PEACE subsea cable systems could provide lower-risk alternative options in the underserved eastern Africa markets. Ensuring development of private and third-party cable routes will also reduce the risk to sensitive data sharing compared with routes such as PEACE. Greater attention to physical protection of CLS facilities and logical protection of data running through the CLS is needed to protect both economic and military interests. Understanding and applying lessons learned about vulnerabilities and risks inherent to end-to-end subsea cable systems, especially in the context of the DSR and PEACE cables, in eastern Africa and their connections to the ICT is critical.

Additional Undersea Cable Resources

Submarine Networks:
www.submarinenetworks.com

Submarine Cable Maps:
www.submarinecablemap.com

Infrapedia Global Internet Infrastructure Maps:
www.infrapedia.com

About the Authors

Nancy Ross is an Infrastructure Engineer in the Cloud, Network, and Digital Service Engineering department of MITRE Labs. Nancy provides technical and leadership expertise on enterprise architecture, network engineering, cloud, and IoT. Prior to joining MITRE, Nancy served as Senior Vice President, Service Operations at Avaya Government Solutions leading government, commercial, and international telecommunications operations.

Maggie Vencill is a Technical Program Manager at the Center for Policy and Strategic Competition. Maggie is an experienced project leader who provides expertise in the area of strategic competition and technology protection to multiple government agencies. Additionally, Maggie is a certified Lean Six Sigma Black Belt with more than 20 years of experience in the commercial and government sectors.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the authors and should not be construed as an official government position, policy, or decision unless designated by other documentation.

Endnotes

[1] Dwayne Winseck, "The Geopolitical Economy of the Global Internet Infrastructure," Journal of Information Policy 7 (2017): 17–18, doi:10.5325/jinfopoli.7.2017.0228; and Tim Stronge, "Does 70% of the World's Internet Traffic Flow through Virginia?," TeleGeography Blog, May 2019, https://blog.telegeography.com/does-70-of-the-worlds-internet-traffic-flow-through-virginia

[2] Opinion: What the Red Sea cable outage should teach us (msn.com) (March 2024) (accessed March 2024)

[3] Decoupling Is Already Happening—Under the Sea – Foreign Policy (May 24, 2023) (accessed March 2024)

[4] PEACE Cable and PCCW Global to leverage Infinera's ICE6 for high-performance PEACE submarine cable system I Virtual-Strategy Magazine (June 8, 2021)

[5] PEACE, PCCW Global and Interxion Reaches a Consensus on Cooperation at the Location of Termination and Interconnection Equipment (peacecable.net/news) (Feb. 5, 2021)

[6] Dr. Daniel Brown, MITRE DSR Economic Study Results: Cables and GDP (August 2021)

[7] B. Lavallee, The Cable Landing Station is Critical Infrastructure, Total Telecom, Feb. 5, 2019 www.totaltele.com/502079/The-cable-landing-station-is-critical-infrastructure

[8] Gil Santaliz, Why the Cable Landing Station Matters, Cable Landing Stations I Pipeline Magazine I Network Evolution (pipelinepub.com) (Accessed March 2024)

[9] P. Morcos and C. Wall, Invisible and Vital: Undersea Cables and Transatlantic Security I Center for Strategic and International Studies (csis.org) (June 11, 2021)

[10] 3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway I AP News (March 4, 2024)

[11] Annual Threat Assessment of the US Intelligence Community, Office of the Director of National Intelligence, April 9, 2021

[12] Cutting the Cord: The Legal Regime Protecting Undersea Cables - Lawfare (lawfareblog.com) (Nov. 21, 2017)

[13] P. Morcos and C. Wall, Invisible and Vital: Undersea Cables and Transatlantic Security I Center for Strategic and International Studies (csis.org) (June 11, 2021)

[14] NIST Special Publication 800-207: Zero Trust Architecture (August 2020)

[15] Africa – Submarine Cable Networks, www.submarinenetworks.com/en/africa (accessed in 2021)

[16] Djibouti City, Djibouti I Cable Landing Station I CLS I Infrapedia (June 23, 2021) (accessed in 2021)

[17] Review of 2021 - Djibouti Telecom (accessed March 2024)

[18] Google Officially Announces Blue and Raman Cable Systems - Submarine Networks (accessed March 2024)

[19] MBA2_Technical-Specification-Sheet.pdf (icolo.io) (accessed March 2024)

[20] PEACE Cable and Telkom land new submarine cable in Kenya - Peace (April 12, 2022)

[21] Terra Firma: Why Terrestrial Connectivity Matters to the Cable Landing Station – NJFX (accessed March 2024)

[22] www.interxion.com/locations/europe/marseille Fact Sheet (accessed in 2021)

[23] PEACE-MED Mediterranean subsea cable section goes live - Peace (peacecable.net) (March 28, 2022)

[24] PEACE, PCCW Global and Interxion Reaches a Consensus on Cooperation at the Location of Termination and Interconnection Equipment (peacecable.net/news) (Feb. 5, 2021)

[25] PEACE Cable Extends to South Africa - Submarine Networks (accessed in 2021)

[26] PEACE submarine cable to land at Interxion's Marseille MRS2 data center - DCD (datacenterdynamics.com) (accessed in 2021)