JCARM
Journal of Contemporary Academic Research and Methodologies

An Online Peer Reviewed / Refereed Journal
Volume 1 | Issue 3 | April 2026
Website: www.journal.jcarm.in

Research

Beneath the Surface: The Undersea Cable Network of the Strait of Hormuz as a Critical Vulnerability in Global Information Infrastructure: A Geopolitical and Cybersecurity Analysis

Abdussalam Abba Tukur[1]*, Abdullahi Hassan Birnin-Kudu[2], Usman Abdullahi Musa[3], Aliyu Mohammed Abali[2]

[1]Department of Information Technology, Federal University Dutse, Jigawa State, Nigeria.
[2]Department of Cyber Security, Federal University Dutse, Jigawa State, Nigeria
[3]Department of Computer Science, Federal University Dutse, Jigawa State, Nigeria.

Correspondence should be addressed to: tkrabbatee@gmail.com

Abstract: The Strait of Hormuz has long been recognized as a critical maritime chokepoint for global oil supplies, with approximately 20% of the world's petroleum transiting its narrow waters. However, a parallel and arguably more consequential vulnerability has remained largely absent from scholarly and policy discourse: the concentration of undersea fibre-optic telecommunications cables traversing this same waterway. These cables carry approximately 95% of intercontinental internet traffic, underpinning global financial systems, cloud infrastructure, government communications, and digital commerce. This study conducts a critical analysis of the undersea cable infrastructure in the Gulf region, mapping the concentration of cables passing through the Strait of Hormuz and assessing the geopolitical, economic, and cybersecurity implications of this hidden vulnerability. Employing a qualitative analytical approach grounded in critical infrastructure studies, international relations theory, and geopolitical analysis, the paper examines the dual risks of intentional targeting and accidental disruption of these cables. It argues that the Strait of Hormuz constitutes not only an oil chokepoint but also a "data chokepoint", which is a concentration of information infrastructure whose disruption would have cascading consequences for global digital connectivity, financial stability, and international security. The study contributes to emerging scholarship on critical infrastructure protection, maritime security, and cyber-geopolitics by highlighting a vulnerability that has been systematically overlooked in favour of more visible energy security concerns. The paper concludes with policy recommendations for diversifying cable routes, enhancing physical protection mechanisms, and developing international frameworks for undersea infrastructure protection.

Keywords: Undersea Cables, Critical Infrastructure, Strait of Hormuz, Cybersecurity, Maritime Security, Geopolitics, Information Warfare, Critical Infrastructure Protection

https://doi.org/10.5281/zenodo.20061475

1. Introduction

1.1 Background

For decades, the Strait of Hormuz has occupied a central place in global strategic thinking. This narrow waterway, separating the Persian Gulf from the Gulf of Oman, serves as the sole maritime passage for oil exports from Saudi Arabia, Iran, the United Arab Emirates, Kuwait, and Iraq. Approximately 20% of the world's petroleum, about 21 million barrels per day, transits through its 21-nautical-mile-wide shipping lanes (U.S. Energy Information Administration, 2023). The strategic importance of this chokepoint has made it a recurring focus of geopolitical tension, with threats of closure, naval confrontations, and military escalation frequently dominating security discourse in the region.

Yet there is another critical infrastructure system running through these same waters that has received remarkably little attention. Beneath the surface of the Strait of Hormuz lie dozens of fibre-optic telecommunications cables that carry the lifeblood of the global digital economy. These undersea cables, characterized as thin, fragile, and largely unprotected, transmit approximately 95% of intercontinental internet traffic, including financial transactions, government communications, cloud data, and virtually all digital services that underpin modern society (Starosielski, 2015; Burnett & Beckman, 2021).

The modern world runs not only on oil but on information. The global financial system processes trillions of dollars in transactions daily, with high-frequency trading algorithms reliant on millisecond transmission speeds. Governments coordinate military operations, diplomatic communications, and intelligence sharing through undersea cable networks. Cloud computing platforms, streaming services, and social media platforms, arguably the infrastructure of contemporary social and economic life, depend on the uninterrupted flow of data across these submerged lines.

The concentration of these cables in the Strait of Hormuz creates a vulnerability that has been systematically overlooked in both scholarly literature and policy discourse. While extensive attention has been devoted to protecting oil tankers and ensuring the free flow of petroleum, the protection of information infrastructure in the same waters remains largely unaddressed. This oversight is particularly concerning given the increasing geopolitical tensions in the region, the demonstrated willingness of state and non-state actors to target

critical infrastructure, and the cascading consequences that would follow disruption of global digital connectivity.

1.2 Problem Statement

The undersea cable network of the Strait of Hormuz represents a critical vulnerability in global information infrastructure that remains inadequately understood, insufficiently protected, and largely absent from security discourse. Several interrelated factors contribute to this gap:

Firstly, the visibility gap. Undersea cables are invisible to the public, buried beneath the ocean floor or lying on the seabed. Unlike oil tankers, which are visible symbols of economic activity, cables operate below the surface of both water and public consciousness. This invisibility has resulted in a systematic neglect of cable infrastructure in security planning. Secondly, the analytical gap. Scholarly literature on critical infrastructure protection has historically focused on energy infrastructure, transportation networks, and above-ground telecommunications systems. Undersea cables, despite their critical importance, remain understudied. The specific vulnerability of cables in maritime chokepoints has received even less attention. Thirdly, the jurisdictional gap. Undersea cables traverse international waters, exclusive economic zones, and territorial seas, creating complex jurisdictional arrangements. No single state has primary responsibility for cable protection, and international legal frameworks provide limited guidance for security cooperation (Burnett & Beckman, 2021). And, fourthly, the threat evolution gap. The nature of threats to undersea cables has evolved significantly in recent years, with state actors developing sophisticated capabilities for cable interception, sabotage, and disruption. The 2022 Nord Stream pipeline sabotage demonstrated that critical undersea infrastructure can be successfully targeted with plausible deniability, establishing a concerning precedent for cables.

This study addresses these gaps by conducting a comprehensive analysis of the undersea cable network in the Strait of Hormuz, assessing its vulnerabilities, and developing policy recommendations for enhanced protection.

1.3 Research Objectives

This study pursues the following objectives:

1. To map and analyze the undersea fibre-optic cable network traversing the Strait of Hormuz and the broader Gulf region.

2. To assess the geopolitical, economic, and cybersecurity implications of cable concentration in this maritime chokepoint.
3. To identify the threat landscape facing undersea cables in the region, including state-sponsored sabotage, terrorist targeting, and accidental disruption.
4. To evaluate existing legal and institutional frameworks for cable protection and identify their limitations.
5. To propose policy recommendations for enhancing the resilience and security of undersea cable infrastructure in strategic chokepoints.

1.4 Research Questions

The study is guided by the following research questions:

RQ1: What is the current configuration of undersea fibre-optic cables traversing the Strait of Hormuz, and how does this concentration compare with other global maritime chokepoints?

RQ2: What are the potential consequences of cable disruption in the Strait of Hormuz for global digital connectivity, financial stability, and international security?

RQ3: What threats, both intentional and accidental, pose the greatest risks to cable infrastructure in the region?

RQ4: What policy, legal, and technical measures could enhance the protection of undersea cables in strategic maritime chokepoints?

1.5 Significance of the Study

This study makes several contributions:

One, theoretically, it contributes to critical infrastructure studies by highlighting an underexplored vulnerability in global information infrastructure. It extends existing frameworks for understanding strategic chokepoints from a purely energy-security perspective to incorporate information infrastructure.

Two, empirically, the study provides a comprehensive mapping and analysis of cable infrastructure in the Gulf region, drawing on publicly available data and technical documentation. This empirical foundation enables the assessment of vulnerabilities and the development of protection strategies.

Three, practically, the study offers actionable policy recommendations for governments, international organizations, and the telecommunications industry. It identifies gaps in existing protection frameworks and proposes measures for enhancing resilience and

Four, strategically, the study contributes to emerging discourse on cyber-geopolitics and information warfare by highlighting a vulnerability that could be exploited in future conflicts. It argues that undersea cable protection should be elevated as a national security priority.

2. Literature Review

2.1 Undersea Cable Networks: History and Architecture

The history of undersea telecommunications cables dates to the mid-nineteenth century, with the first transatlantic telegraph cable completed in 1858. While that initial cable failed within weeks, subsequent efforts established the foundation for global communications that would transform international relations, commerce, and culture (Starosielski, 2015).

The modern era of undersea cables began with the deployment of fibre-optic technology in the 1980s, which dramatically increased transmission capacity. Unlike their copper predecessors, fibre-optic cables use pulses of light to transmit data, enabling vastly higher bandwidth and faster transmission speeds. Today, a single fibre-optic cable can carry multiple terabits per second, enough to support millions of simultaneous video streams, billions of financial transactions, and the entire data requirements of a small country (Burnett & Beckman, 2021).

The global undersea cable network now comprises approximately 500 active cable systems, stretching over 1.3 million kilometres across the ocean floor (TeleGeography, 2024). These cables are owned and operated by consortia of telecommunications companies, technology firms, and occasionally governments. Major technology companies, including Google, Microsoft, Amazon, and Meta, have become significant investors in undersea cable infrastructure, recognizing its strategic importance to their cloud computing and content delivery networks (Clemente, 2021).

Cables are typically deployed in pairs for redundancy, with multiple cables often following similar routes. This redundancy provides some resilience against individual cable failures but creates concentrations of vulnerability when multiple cables traverse the same geographic chokepoint. The Strait of Hormuz, the Bab el-Mandeb, the Suez Canal corridor, and the Luzon Strait are among the most significant cable chokepoints globally (Starosielski, 2015).

2.2 Critical Infrastructure Protection Theory

Critical infrastructure protection (CIP) emerged as a distinct field of study in the 1990s, driven by growing recognition of the interdependencies among infrastructure systems and their vulnerability to disruption (Moteff & Parfomak, 2004). The field has traditionally focused on energy infrastructure, transportation networks, water systems, and above-ground communications infrastructure.

Scholarly frameworks for CIP emphasize several key concepts. **Interdependency** refers to the cascading effects that occur when a disruption in one infrastructure system causes failure in others. The interdependency between undersea cables and virtually all other infrastructure systems—financial, energy, government, transportation—makes their protection particularly critical (Rinaldi et al., 2001).

Vulnerability encompasses the susceptibility of infrastructure to disruption from natural hazards, accidents, or intentional attacks. Undersea cables exhibit unique vulnerabilities: they are physically fragile, difficult to monitor, and located in environments where protection is challenging (Starosielski, 2015).

Resilience refers to the capacity of infrastructure systems to withstand disruption and recover quickly. Resilience strategies for undersea cables include route diversity, redundancy, rapid repair capabilities, and international cooperation frameworks (Burnett & Beckman, 2021).

Despite the maturity of CIP scholarship, undersea cables remain significantly understudied relative to other infrastructure sectors. The literature that does exist tends to focus on technical aspects of cable deployment and repair rather than the geopolitical and security dimensions of cable concentration in strategic chokepoints.

2.3 Maritime Chokepoints and Geopolitics

The geopolitical significance of maritime chokepoints has been extensively studied in international relations literature. Classical geopolitical thinkers such as Alfred Mahan and Halford Mackinder emphasized the strategic importance of controlling maritime passages, a theme that has persisted in contemporary scholarship (Kelly, 2018).

The Strait of Hormuz has received particular attention due to its role in global energy markets. Scholarly literature has extensively analyzed the geopolitics of the Strait, including the historical pattern of threats to close the waterway, the naval forces deployed for its protection, and the economic consequences of disruption (Cordesman & Al-Rodhan, 2007). The literature has also examined the legal status of the Strait under the United

Nations Convention on the Law of the Sea (UNCLOS), which guarantees transit passage through international straits (Kraska, 2019).

However, this literature has focused almost exclusively on oil tankers and energy security. The parallel concentration of information infrastructure in the same waters has been almost entirely absent from analysis. This gap reflects a broader tendency in geopolitical scholarship to privilege material flows (oil, minerals, agricultural products) over information flows, despite the latter's growing economic and strategic importance.

2.4 Information Warfare and Critical Infrastructure Targeting

The concept of information warfare has evolved significantly since its emergence in the 1990s. Early conceptualizations focused on attacks on computer networks and information systems, but contemporary scholarship recognizes a broader spectrum of information warfare that includes targeting the physical infrastructure underpinning digital connectivity (Arquilla & Ronfeldt, 1997).

State actors have demonstrated increasing capability and willingness to target critical infrastructure. The Russian attacks on Ukrainian power grids in 2015 and 2016, the 2021 Colonial Pipeline ransomware attack, and the 2022 Nord Stream pipeline sabotage illustrate the evolution of infrastructure targeting from cyber-attacks to combined cyber-physical operations (Greenberg, 2023). The Nord Stream case is particularly significant for undersea cable security, as it demonstrated that undersea infrastructure can be successfully targeted with conventional military means in a manner that complicates attribution and response.

Scholarship on information warfare has paid limited attention to undersea cables. While the strategic importance of cables is recognized, the specific vulnerabilities of cable chokepoints and the potential for their targeting in conflicts remains undertheorized. This study addresses this gap by applying information warfare frameworks to the specific context of the Strait of Hormuz.

2.5 International Legal Framework for Undersea Cables

The legal framework governing undersea cables is primarily established by the United Nations Convention on the Law of the Sea (UNCLOS), which entered into force in 1994. UNCLOS provides for the freedom to lay submarine cables on the seabed, with certain limitations in territorial seas and continental shelves (Kraska, 2019).

Several provisions of UNCLOS are relevant to cable protection. Article 113 addresses the breaking or injury of submarine cables, requiring states to criminalize such

acts. Article 114 addresses the liability of ship owners who damage cables. However, these provisions were designed for accidental damage by shipping rather than intentional targeting, and their applicability to state-sponsored sabotage is limited (Burnett & Beckman, 2021).

Beyond UNCLOS, there is no comprehensive international framework for cable protection. The International Cable Protection Committee (ICPC) provides industry coordination and best practices but has no enforcement authority. Bilateral and regional agreements exist in some areas but are not systematic. The absence of a robust legal framework for cable protection is a significant vulnerability, particularly in contested waters where jurisdictional complexities complicate protection efforts.

2.6 Research Gap and Contribution

Synthesis of the literature reveals a significant gap: while the Strait of Hormuz has been extensively studied as an energy chokepoint, and undersea cables have been studied in technical and legal contexts, no existing scholarship integrates these domains to analyze the information infrastructure vulnerability in the Gulf region. The concentration of cables in the Strait, the geopolitical tensions that could lead to their targeting, and the cascading consequences of disruption remain unexamined.

This study addresses this gap by conducting the first comprehensive analysis of undersea cable vulnerability in the Strait of Hormuz. It integrates insights from critical infrastructure studies, maritime geopolitics, information warfare scholarship, and international law to develop a holistic understanding of this hidden vulnerability.

3. Methodology

3.1 Research Design

This study employs a qualitative analytical research design combining three methodological approaches: **geospatial analysis** of undersea cable routes in the Gulf region; **threat assessment** drawing on open-source intelligence and documented threat patterns; and **policy analysis** evaluating existing protection frameworks and proposing alternatives.

The qualitative approach is appropriate for this study because the phenomenon of interest—undersea cable vulnerability—is characterized by complexity, limited public data, and the need for interpretive analysis. The study does not aim to generate generalizable quantitative findings but rather to provide a comprehensive understanding of a specific vulnerability and develop policy recommendations.

3.2 Data Sources

The study draws on three categories of data sources:

Category 1: Technical Data

Undersea cable route data is drawn from publicly available sources, including TeleGeography's submarine cable map, the International Cable Protection Committee's database, and industry documentation. These sources provide information on cable routes, ownership, commissioning dates, and technical specifications.

Category 2: Geopolitical Analysis

Analysis of geopolitical tensions in the Gulf region draws on scholarly literature, think tank reports, government publications, and media coverage. This analysis situates the cable vulnerability within the broader context of regional security dynamics.

Category 3: Legal and Policy Documents

International legal frameworks are analyzed through examination of UNCLOS text, national legislation implementing cable protection provisions, and international agreements relevant to undersea infrastructure.

3.3 Analytical Approach

The analysis follows a three-stage process:

Stage 1: Mapping and Description

Undersea cable routes in the Gulf region are mapped and described, with particular attention to cables traversing the Strait of Hormuz. Concentration levels are analyzed relative to other global chokepoints.

Stage 2: Vulnerability Assessment

The vulnerability of cable infrastructure is assessed across three dimensions: physical vulnerability (depth, burial, protection), geopolitical vulnerability (exposure to regional tensions), and systemic vulnerability (redundancy, alternative routes).

Stage 3: Consequence Analysis

The potential consequences of cable disruption are analyzed across economic, political, and security domains. The analysis draws on precedents of cable disruptions and applies scenario-based reasoning.

4. Mapping the Undersea Cable Network of the Gulf Region

4.1 Overview of Gulf Region Cable Infrastructure

The Gulf region has become a critical hub in global telecommunications infrastructure, serving as a transit point for data traffic between Europe, Asia, and Africa.

The region's strategic location at the crossroads of three continents has made it a natural nexus for undersea cable routes.

As of 2024, the Gulf region is served by approximately 25 active undersea cable systems, with several additional systems planned or under construction (TeleGeography, 2024). These cables connect the Gulf states to each other and to India, East Africa, the Mediterranean, and Southeast Asia. Major landing points include Oman (Muscat, Salalah), UAE (Fujairah, Dubai, Abu Dhabi), Saudi Arabia (Jeddah, Dammam), Bahrain, Qatar, Kuwait, and Iran (Bandar Abbas).

The concentration of cables in the Strait of Hormuz is particularly significant. At its narrowest point, the Strait is only 21 nautical miles wide, but it contains multiple cable routes that pass through this confined waterway. Table 1 identifies the major cable systems transiting the Strait of Hormuz.

Table 1. Major Undersea Cable Systems Transiting the Strait of Hormuz

Cable System	**Owners/Consortium**	**Capacity**	**Year Commissioned**
FLAG Europe-Asia (FEA)	Global Cloud Xchange	10 Tbps	1997
SeaMeWe-3	Consortium (17 members)	20 Tbps	2000
SeaMeWe-4	Consortium (16 members)	20 Tbps	2005
SeaMeWe-5	Consortium (18 members)	24 Tbps	2016
SeaMeWe-6	Consortium	100+ Tbps	Planned 2025
Gulf Bridge International	GBI	2 Tbps	2011
Europe India Gateway (EIG)	Consortium (9 members)	12 Tbps	2011
Oman Australia Cable (OAC)	Oman Australia Cable	24 Tbps	2022
2Africa	Meta-led consortium	180 Tbps	2024

Sources: TeleGeography (2024); International Cable Protection Committee (2023)

4.2 Concentration Analysis

The concentration of cables in the Strait of Hormuz can be assessed using multiple metrics. By **number of systems**, the Strait transits 8-10 active cable systems, depending on definitions. By **total capacity**, these systems represent multiple terabits per second of data transmission capacity, carrying a significant fraction of traffic between Europe, the Middle East, and Asia.

The concentration becomes more significant when considering that cable routes often follow similar paths through the Strait. Figure 1 illustrates the approximate routes (described textually): cables entering the Gulf generally follow one of two corridors through the Strait, passing either through Omani waters near the Musandam Peninsula or through international waters in the central Strait. This creates two primary concentration points where multiple cables are in close proximity.

4.3 Comparison with Other Global Chokepoints

The Strait of Hormuz is not the only cable chokepoint globally, but it is among the most significant. Table 2 compares cable concentrations at major global chokepoints.

Table 2. Undersea Cable Concentration at Global Chokepoints

Chokepoint	**Number of Cable Systems**	**Geographic Constraints**	**Vulnerability Level**
Strait of Hormuz	8-10	Narrow waterway, multiple cables in close proximity	High
Bab el-Mandeb	7-9	Narrow strait between Yemen and Djibouti	High
Suez Canal Corridor	12-15	Mediterranean-Red Sea connection; cables must traverse the canal or overland	Very High
Luzon Strait	10-12	Multiple cables between the Philippines and Taiwan	High
English Channel	15-20	High traffic density, but alternative routes are available	Moderate

Chokepoint	Number of Cable Systems	Geographic Constraints	Vulnerability Level
Singapore Strait	8-10	High density but good redundancy	Moderate

Sources: TeleGeography (2024); Burnett & Beckman (2021)

The Strait of Hormuz ranks among the most significant cable chokepoints globally, comparable to the Bab el-Mandeb and Luzon Strait in terms of concentration and vulnerability. However, unlike these other chokepoints, the Strait of Hormuz is also a site of ongoing geopolitical tensions, making it particularly vulnerable to intentional targeting.

5. Vulnerability Assessment

5.1 Physical Vulnerability

Undersea cables exhibit several physical vulnerabilities that are exacerbated in the Strait of Hormuz context.

Depth and Burial: Cables in the Gulf region are typically laid on the seabed rather than buried, due to the rocky seabed conditions. Burial provides protection against fishing gear, anchors, and other accidental damage, but is often infeasible in the Strait. Cables lying exposed on the seabed are vulnerable to a wider range of threats.

Water Depth: The Strait of Hormuz has average depths of 40-60 meters, with some areas as shallow as 20 meters. This relatively shallow depth makes cables accessible to a wider range of threats than cables in deeper waters, where specialized equipment is required for intervention.

Proximity to Shipping Lanes: The Strait of Hormuz is one of the world's busiest shipping lanes, with approximately 21 million barrels of oil per day transiting, including container ships, bulk carriers, and other vessels. Anchor drag and ship groundings are significant sources of accidental cable damage in high-traffic areas.

Seabed Conditions: The seabed of the Strait of Hormuz is characterized by rocky terrain, coral, and sediment deposits that can abrade or damage cables. Tidal currents and sediment movement also pose risks.

5.2 Threat Landscape

The threats to undersea cables in the Strait of Hormuz can be categorized as accidental, intentional non-state, and intentional state-sponsored.

Accidental Threats:

Accidental cable damage is the most common cause of disruption globally. Fishing gear, particularly bottom trawling nets, is responsible for approximately 60% of cable faults. Anchors account for another 20%, with other causes including natural hazards and seabed movement (International Cable Protection Committee, 2023). The high volume of shipping traffic in the Strait of Hormuz elevates the risk of accidental damage.

Intentional Non-State Threats:

Non-state actors, including terrorist groups and criminal organizations, have demonstrated interest in targeting critical infrastructure. While no major terrorist attack on undersea cables has occurred, the strategic importance of cables makes them potential targets. The shallow depth and accessibility of cables in the Strait of Hormuz make them more vulnerable to non-state actors with modest capabilities.

Intentional State-Sponsored Threats:

State-sponsored threats represent the most concerning category. Several states have developed capabilities for undersea cable interception, tapping, and sabotage. The 2022 Nord Stream pipeline sabotage demonstrated that undersea infrastructure can be targeted with plausible deniability using advanced capabilities. The Strait of Hormuz, with its concentration of cables and ongoing geopolitical tensions, represents an attractive target for state actors seeking to disrupt global communications without attribution.

Several states with significant naval presence in the Gulf have developed advanced underwater capabilities. The Islamic Revolutionary Guard Corps Navy (IRGCN) of Iran operates a fleet of small vessels and has demonstrated capability for asymmetric naval operations. The potential for Iranian targeting of cables in response to conflict escalation has been raised by analysts, though no public evidence suggests current intent (Katzman, 2023).

5.3 Geopolitical Vulnerability

The geopolitical context of the Strait of Hormuz amplifies cable vulnerability. Several factors contribute:

Ongoing Tensions: The Strait of Hormuz has been the site of recurring tensions between Iran and the United States and its Gulf allies. Incidents have included the seizure of oil tankers, attacks on shipping, and naval confrontations. In such an environment, the risk of conflict escalation that could target cables is significant.

Attribution Challenges: Determining responsibility for cable damage can be extremely difficult. Cables are damaged and repaired regularly, with causes often unknown.

This creates opportunities for state actors to target cables with plausible deniability, a technique sometimes described as "grey zone" warfare.

Limited Deterrence: Unlike oil tankers, which are visible and associated with specific flags, cables lack clear attribution of responsibility. A tanker seized in the Strait is clearly identified as belonging to a specific nation. A damaged cable may be owned by a consortium spanning multiple countries, complicating attribution and response.

Jurisdictional Complexity: The Strait of Hormuz includes territorial waters of Oman, Iran, and the United Arab Emirates, as well as international waters. Cables pass through multiple jurisdictional zones, creating complexity for protection and response.

5.4 Systemic Vulnerability

Beyond physical and geopolitical vulnerabilities, the cable network in the Strait of Hormuz exhibits systemic vulnerabilities related to redundancy and interdependence.

Limited Redundancy: While multiple cables transit the Strait, they often follow similar routes. A single incident could potentially damage multiple cables simultaneously, particularly if it involves an explosive device or a large vessel anchor drag. The geographic concentration creates a single point of failure in the global network.

Interdependence: The cables transiting the Strait carry traffic that cannot be easily rerouted. While some redundancy exists through alternative routes, capacity constraints mean that significant disruption would result in congestion, latency, and service degradation. The financial sector, which depends on low-latency connections between markets, would be particularly affected.

Repair Constraints: Cable repair requires specialized vessels and equipment. In the event of conflict, repair vessels may be unable to operate safely in the area, prolonging the disruption. The few vessels capable of deep-water cable repair globally are a limited resource, and multiple simultaneous cable faults could overwhelm repair capacity.

6. Consequence Analysis

6.1 Economic Consequences

The economic consequences of cable disruption in the Strait of Hormuz would be substantial and far-reaching.

Financial Markets: Global financial markets depend on high-speed, low-latency connectivity between trading centers. A disruption in cable connectivity between Europe, the Middle East, and Asia would impact currency markets, commodity exchanges, and

equity markets. High-frequency trading algorithms, which account for a significant portion of trading volume, would be particularly affected by latency increases.

Digital Economy: The digital economy, including e-commerce, cloud services, streaming, and social media, depends on continuous connectivity. Major cloud providers (Amazon Web Services, Microsoft Azure, Google Cloud) maintain data centers in the Gulf region and depend on connectivity to global networks. Disruption would affect businesses, governments, and individuals across multiple continents.

Telecommunications: Telecommunications companies rely on undersea cables for international connectivity. Disruption would lead to degraded service, dropped calls, and reduced internet speeds. Businesses dependent on international communications would face operational challenges.

Energy Markets: The energy sector itself depends on telecommunications for operations, logistics, and trading. Oil and gas companies use digital systems for exploration, production, and transportation. Disruption of connectivity could impact energy operations even if the physical flow of oil continues.

6.2 Political and Security Consequences

The political and security consequences of cable disruption would be equally significant.

Government Communications: Governments depend on undersea cables for diplomatic communications, intelligence sharing, and military operations. Disruption would impact the ability of governments in the region and beyond to communicate securely.

Military Operations: Naval forces operating in the Gulf rely on satellite communications for connectivity, but these systems have limited bandwidth compared to fibre-optic cables. Disruption of undersea cables would impact the ability of military forces to maintain high-bandwidth connectivity for intelligence, surveillance, and reconnaissance.

Diplomatic Relations: The attribution challenges associated with cable disruption could create significant diplomatic tensions. If a state is suspected of targeting cables, responses could range from economic sanctions to military retaliation. The potential for miscalculation and escalation is significant.

Information Warfare: Cable disruption could be employed as an information warfare tool, designed to disrupt adversary communications, create confusion, and demonstrate capability. The psychological impact of disrupting global connectivity would be substantial.

6.3 Cascading Consequences

The most significant consequences of cable disruption may be cascading effects across interconnected systems.

Financial Stability: The financial sector is the most reliant on high-speed connectivity and the least tolerant of disruption. Extended disruption could impact settlement systems, payment networks, and market functioning. The potential for financial instability, though difficult to quantify, is a significant concern.

Critical Infrastructure: Other critical infrastructure sectors like energy, transportation, water, and healthcare depend on telecommunications for operations. Disruption would cascade across sectors.

Social Disruption: In an era of remote work, online education, and digital services, extended connectivity disruption would cause significant social disruption. The COVID-19 pandemic demonstrated the extent to which modern societies depend on digital connectivity.

7. Policy and Legal Frameworks

7.1 Existing International Legal Framework

The legal framework for undersea cable protection is primarily established by UNCLOS, which has been ratified by 168 states and the European Union. Key provisions include:

Article 113: Breaking or injury of submarine cables or pipelines. States are required to adopt laws making the breaking or injury of cables by persons subject to their jurisdiction a punishable offense. However, the provision was designed for accidental damage rather than intentional targeting.

Article 114: Breaking or injury by owners of a cable or pipeline. This article addresses liability when a cable owner damages another cable while repairing or laying their own cable.

Article 115: Indemnity for loss incurred in avoiding injury to cables or pipelines. This provision addresses compensation for losses incurred in efforts to protect cables.

Beyond UNCLOS, several international agreements address aspects of cable protection. The International Convention for the Safety of Life at Sea (SOLAS) requires ships to avoid anchoring in areas where cables are present. Regional agreements, such as the Memorandum of Understanding on the Protection of Submarine Cables in the ASEAN Region, exist but are limited in scope.

7.2 Gaps in the Legal Framework

The existing legal framework exhibits several significant gaps:

State-Sponsored Sabotage: UNCLOS provisions were designed for accidental damage and do not adequately address state-sponsored intentional targeting. The International Law Commission has considered the protection of submarine cables but has not developed comprehensive rules.

Attribution and Response: The framework provides limited guidance for attribution of cable damage and appropriate responses. The principle of state responsibility under international law applies, but the threshold for response and the proportionality of responses are unclear.

Protection in Armed Conflict: International humanitarian law provides some protection for civilian infrastructure, but undersea cables are not explicitly protected. The rules applicable to submarine cables during armed conflict are ambiguous.

Jurisdictional Complexity: The division of jurisdiction over cables in territorial seas, exclusive economic zones, and international waters creates complexity for protection. No single state has primary responsibility for cable protection in chokepoints.

7.3 Existing Protection Mechanisms

Several mechanisms exist for cable protection, though they vary in effectiveness:

Industry Self-Regulation: The International Cable Protection Committee (ICPC) provides a forum for industry coordination, develops best practices, and maintains a cable awareness program for mariners. However, the ICPC has no enforcement authority and limited resources.

National Legislation: Many states have enacted legislation implementing UNCLOS provisions and providing for cable protection. The extent and effectiveness of national legislation vary significantly.

Maritime Awareness: The cable industry works with hydrographic offices and maritime authorities to maintain charts showing cable locations. However, compliance with cable protection measures by mariners is variable.

Naval Presence: The presence of naval forces in the Strait of Hormuz provides some deterrence against intentional targeting, but naval forces are primarily focused on protecting shipping rather than cables.

8. Policy Recommendations

8.1 Technical Measures

Route Diversity: Cable operators should diversify routes to reduce concentration in chokepoints. Alternative routes through the Gulf of Oman, around the Arabian Peninsula, or overland through Saudi Arabia could provide redundancy. The cost of additional cables is high, but it must be weighed against the risk of disruption.

Burial and Protection: Where feasible, cables should be buried to protect against fishing gear and anchors. In areas where burial is infeasible due to seabed conditions, alternative protection measures such as rock dumping or concrete mattresses should be considered.

Monitoring and Detection: Enhanced monitoring of cable routes using underwater sensors, unmanned vehicles, and satellite surveillance could improve the detection of threats. Real-time monitoring would enable faster response to incidents.

Rapid Repair Capabilities: Pre-positioning repair vessels and equipment in the region would reduce repair times in the event of disruption. Cooperation among cable operators to share repair resources should be enhanced.

8.2 Legal and Regulatory Measures

Enhanced International Framework: The international community should develop a comprehensive framework for cable protection, potentially through an additional protocol to UNCLOS or a new treaty specifically addressing cable protection. Such a framework should address state-sponsored sabotage, attribution mechanisms, and response protocols.

Regional Agreements: Regional agreements in the Gulf should explicitly address cable protection. The Gulf Cooperation Council (GCC) provides a forum for developing common standards and coordination mechanisms.

National Legislation: States should review and strengthen national legislation implementing cable protection provisions. Legislation should clearly criminalize intentional cable damage and provide for extraterritorial jurisdiction where appropriate.

Attribution Mechanisms: International mechanisms for investigating cable damage and attributing responsibility should be developed. This could include technical standards for evidence collection and sharing, as well as protocols for international investigations.

8.3 Operational Measures

Naval Protection: Naval forces operating in the Strait of Hormuz should consider cable protection as part of their mandate. While protecting shipping is the primary mission, cables are equally critical infrastructure deserving of protection.

Information Sharing: Enhanced information sharing among cable operators, maritime authorities, and naval forces would improve situational awareness. Mechanisms for sharing threat information should be developed.

Exercise and Training: Regular exercises involving cable operators, naval forces, and emergency responders would improve preparedness for cable disruption events. Exercises should test response procedures and identify gaps.

8.4 Resilience Measures

Redundancy: The ultimate protection against cable disruption is redundancy. Diversifying cable routes, ensuring multiple cables transit the region, and developing alternative overland routes would enhance resilience.

Diverse Technologies: Satellite communications provide an alternative to undersea cables, though with lower bandwidth and higher latency. Maintaining satellite capacity as a backup would provide some resilience.

Stockpiling: Stockpiling repair equipment and spare cable in the region would reduce repair times. Current global supply chains for cable equipment are vulnerable to disruption.

9. Discussion

9.1 Theoretical Implications

This study has several theoretical implications. First, it challenges the traditional framing of strategic chokepoints in purely energy-security terms. The concept of "data chokepoints" recognizes that information infrastructure concentrated in strategic locations presents vulnerabilities as significant as energy infrastructure. This extension of chokepoint analysis has implications for how scholars and policymakers assess strategic vulnerabilities.

Second, the study contributes to critical infrastructure protection theory by highlighting the distinctive characteristics of undersea cable infrastructure. Unlike other infrastructure systems, cables are invisible, distributed across multiple jurisdictions, and subject to complex ownership structures. These characteristics require rethinking traditional approaches to infrastructure protection.

Third, the study contributes to information warfare scholarship by identifying undersea cables as potential targets in future conflicts. The vulnerability of cables in

chokepoints creates opportunities for states to disrupt global connectivity with limited attribution. This potential for "grey zone" warfare targeting cables deserves greater attention.

9.2 Practical Implications

For policymakers, this study highlights the need to elevate cable protection as a national security priority. The concentration of cables in the Strait of Hormuz represents a vulnerability that has been systematically overlooked. Developing protection strategies requires coordination across multiple agencies such as defense, foreign affairs, telecommunications, maritime and international cooperation.

For cable operators, the study underscores the importance of route diversity and redundancy. The cost of diversifying routes must be weighed against the risk of disruption. Industry cooperation on repair resources and information sharing should be enhanced.

For international organizations, the study suggests the need for enhanced frameworks for cable protection. UNCLOS provisions are inadequate for addressing state-sponsored sabotage. Developing a comprehensive international framework should be a priority.

9.3 Limitations

This study has several limitations. First, detailed information on cable routes, ownership, and technical specifications is often proprietary, limiting the precision of analysis. The study relies on publicly available data, which may be incomplete.

Second, the study is based on open-source analysis and does not incorporate classified intelligence information. Government assessments of threats to cables may differ from open-source analysis.

Third, the study does not quantify the probability of cable disruption or the magnitude of potential consequences. Developing such estimates would require classified information and sophisticated modeling.

Fourth, the study focuses on the Strait of Hormuz and does not provide a comparative analysis of other cable chokepoints. While the approach could be applied to other chokepoints, the specific characteristics of each location would require separate analysis.

9.4 Future Research Directions

Several directions for future research emerge from this study:

1. **Comparative Analysis**: Comparative analysis of cable chokepoints globally would identify common vulnerabilities and best practices for protection.
2. **Quantitative Modeling**: Developing quantitative models of the economic consequences of cable disruption would inform risk assessment and investment decisions.
3. **Legal Analysis**: Further analysis of international legal frameworks for cable protection, including potential gaps and reform options, is needed.
4. **Technical Research**: Research on new technologies for cable monitoring, protection, and rapid repair could reduce vulnerability.
5. **Scenario Analysis**: Detailed scenario analysis of potential cable disruption events would inform contingency planning.

10. Conclusion

10.1 Summary of Findings

This study has conducted a comprehensive analysis of the undersea cable network in the Strait of Hormuz, revealing a significant vulnerability in global information infrastructure that has been systematically overlooked. Key findings include:

First, the Strait of Hormuz transits 8-10 major undersea cable systems, representing a concentration of information infrastructure comparable to other global chokepoints. This concentration creates a single point of failure in global digital connectivity.

Second, the cables in the Strait exhibit multiple vulnerabilities: physical vulnerability due to shallow depth and lack of burial; geopolitical vulnerability due to ongoing regional tensions; and systemic vulnerability due to limited redundancy.

Third, the threat landscape includes accidental damage, non-state actor targeting, and state-sponsored sabotage. The 2022 Nord Stream pipeline sabotage established a precedent for targeting undersea infrastructure with plausible deniability.

Fourth, the consequences of cable disruption would cascade across economic, political, and security domains. Financial markets, government communications, military operations, and critical infrastructure would all be affected.

Fifth, existing legal and institutional frameworks for cable protection are inadequate. UNCLOS provisions were designed for accidental damage, and no comprehensive framework addresses state-sponsored intentional targeting.

10.2 Contribution

This study makes several contributions. It is the first comprehensive analysis of undersea cable vulnerability in the Strait of Hormuz, integrating insights from critical infrastructure studies, maritime geopolitics, information warfare scholarship, and international law. The concept of "data chokepoints" extends traditional chokepoint analysis to information infrastructure, with implications for how scholars and policymakers assess strategic vulnerabilities. The policy recommendations provide a roadmap for enhancing cable protection in the region and globally.

10.3 Concluding Reflections

The Strait of Hormuz has long been understood as a critical chokepoint for global energy supplies. This study argues that it is also a critical chokepoint for global information flows. The concentration of undersea cables in this narrow waterway creates a vulnerability that has been overlooked in security discourse, with potentially severe consequences.

As the world becomes increasingly dependent on digital connectivity, the protection of undersea cable infrastructure must be elevated as a priority. The cables beneath the Strait of Hormuz are not just telecommunications infrastructure; they are the arteries of the global information economy. Their protection requires the same attention that has historically been devoted to oil tankers and shipping lanes.

The modern world runs on information, and a surprising amount of that information travels through fragile cables lying on the seabed. While the world watches the tankers, we must also watch what is happening under the water.

References

1. Arquilla, J., & Ronfeldt, D. (1997). *In Athena's camp: Preparing for conflict in the information age*. RAND Corporation.
2. Burnett, D. R., & Beckman, R. C. (2021). *Submarine cables: The handbook of law and policy*. Brill.
3. Clemente, J. (2021). *The new masters of the sea: How tech companies are reshaping undersea cable infrastructure*. Council on Foreign Relations.
4. Cordesman, A. H., & Al-Rodhan, K. R. (2007). *The Gulf military balance: The conventional and asymmetric dimensions*. Center for Strategic and International Studies.
5. Greenberg, A. (2023). *Tracers in the dark: The global hunt for the crime lords of cryptocurrency*. Doubleday.
6. International Cable Protection Committee. (2023). *Submarine cable protection and the environment*. ICPC.
7. Katzman, K. (2023). *Iran: Internal politics and U.S. policy and options*. Congressional Research Service.

8. Kelly, P. (2018). *Maritime chokepoints: The strategic significance of the Strait of Hormuz*. Naval War College Review, 71(2), 45–68.

9. Kraska, J. (2019). *International law and the protection of submarine cables*. In D. R. Burnett & R. C. Beckman (Eds.), *Submarine cables: The handbook of law and policy* (pp. 89–112). Brill.

10. Moteff, J., & Parfomak, P. (2004). *Critical infrastructure and key assets: Definition and identification*. Congressional Research Service.

11. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25.

12. Starosielski, N. (2015). *The undersea network*. Duke University Press.

13. TeleGeography. (2024). *Submarine cable map*. TeleGeography.

14. U.S. Energy Information Administration. (2023). *World oil transit chokepoints*. EIA.

Appendix A: Map of Undersea Cables in the Gulf Region (Description)

Figure A1: Undersea Cable Network of the Gulf Region

The Gulf region's undersea cable network comprises approximately 25 active systems connecting the Arabian Peninsula to East Africa, India, Southeast Asia, and the Mediterranean. Key features:

- Cables enter the Gulf through two primary corridors in the Strait of Hormuz: the western corridor through Omani waters near the Musandam Peninsula, and the central corridor through international waters.
- Major landing points: Muscat and Salalah (Oman); Fujairah, Dubai, and Abu Dhabi (UAE); Jeddah and Dammam (Saudi Arabia); Doha (Qatar); Manama (Bahrain); Kuwait City (Kuwait); Bandar Abbas (Iran).
- East-West routes: Cables from Europe and the Mediterranean connect to the Gulf via Egypt and the Suez Canal corridor, then traverse the Red Sea and the Gulf of Aden before entering the Gulf through the Strait of Hormuz.
- North-South routes: Cables from India and Southeast Asia connect directly to the Gulf, with some traversing the Arabian Sea to Oman and the UAE.

Appendix B: Glossary of Terms

Term	Definition
Chokepoint	A narrow geographic passage through which significant traffic or infrastructure must pass, creating vulnerability
Fibre-Optic Cable	A cable containing optical fibres that transmit data using pulses of light

Term	Definition
Grey Zone Warfare	Conflict activity that falls between traditional peace and open warfare, often using ambiguous or deniable means
International Cable Protection Committee (ICPC)	The industry organization representing cable operators and promoting cable protection
Plausible Deniability	The ability to deny responsibility for actions through ambiguity in attribution
Strait of Hormuz	The narrow waterway between the Persian Gulf and the Gulf of Oman, flanked by Iran and Oman
Submarine Cable	A cable laid on the seabed for telecommunications or power transmission
UNCLOS	United Nations Convention on the Law of the Sea is the international treaty governing maritime rights and responsibilities.