

Securing the Digital Seabed

Countering China's Underwater Ambitions

RAGHVENDRA KUMAR

Abstract

China's Digital Silk Road provides Beijing with a potent instrument to disrupt undersea cables and gain an advantage in the Indo-Pacific. Submarine fiber-optic cables are critical infrastructure yet vulnerable to sabotage. This paper examines how the planned Pakistan and East Africa Connecting Europe (PEACE) cable from China could become a new flashpoint in the Western Indian Ocean. The cable has strategic implications, allowing China to project power and leverage its technological edge. Its landing sites in Pakistan and Djibouti would anchor Chinese naval assets in key chokepoints. The civil-military fusion strategy also facilitates surveillance and espionage via the cables. To counter such threats, India and allies must secure submarine cables through monitoring, contingency planning, and multilateral cooperation. Investing in alternative "democratic digital networks" can also mitigate China's ambitions. Ultimately, submarine cables are emerging as a domain of geopolitical competition requiring policies that safeguard their resilience.

The Indian Ocean is becoming a major theater of geopolitical contest for strategic dominance in the wider Indo-Pacific. The Western Indian Ocean (WIO), in particular, has emerged as the strategic center stage for great-power games. This region comprises the Persian Gulf, Arabian Sea, Red Sea, and critical straits of Bab-el-Mandeb, Hormuz, and Suez Canal. It is the key entry point for major powers and plays a vital role in geostrategic calculations given its transit route significance for trade, energy security, and submarine data cables. The WIO's cables are intricately linked to Indo-Pacific geopolitical dynamics and rivalries among regional nations. As the hub connecting Europe, Asia, and Africa, the WIO's critical technology infrastructure for undersea data cables is essential in shaping power dynamics. The evolving security dynamics necessitate examining cable protection and security as an ongoing interest. This article highlights Indian and global efforts to secure critical technologies infrastructure as national security strategy. It examines cable geosecurity dynamics in the WIO's "great game" and India's counterstrategies to contain China's technology push for geopolitical gains.

Submarine Data Cables

Submarine cables and pipelines constitute critical infrastructure for transporting energy (including gas, oil, and electricity) and telecommunications. *Submarine data cables*, defined as “means of communication laid on the seabed between two terminal points,”¹ can be categorized into two types: power cables, responsible for transmitting energy, and data cables, facilitating the transmission of Internet, voice, and data.² In the realm of promoting telecommunications and international communications, the concept of freedom of the seas takes center stage, with the installation of underwater data cables emerging as a pivotal component. These submarine data cables are strategically placed on the ocean floor, connecting land-based stations, and play a vital role in carrying voice and data traffic worldwide, serving multiple purposes.

In the modern era, these data cables have become the linchpin of the global economy and a cornerstone of national security strategy. The growing dependence of societies on the Internet for daily life underscores the necessity for a comprehensive understanding of the framework underpinning the security of these critical electronic communication systems. Presently, fiber-optic cable-based systems are increasingly preferred for day-to-day data transmission, offering not only cost-efficiency but also significantly faster data and voice transfer compared to satellite alternatives. Their applications extend to various domains, encompassing marine scientific data collection, underwater oceanographic research, digital mapping of oil and gas exploration sites, among others.³

The Information and Communication Technology Revolution and Modern-day Conflict

The information and communication technology (ICT) revolution, post–Cold War, has assumed a role that can potentially exacerbate modern-day conflicts. The concept of *hybrid warfare*, characterized by the smart and innovative utilization of

¹ Lionel Carter et al., *Submarine Cables and the Oceans: Connecting the World* (Cambridge, UK: United Nations Environment Programme, 2009).

² Tara Davenport, “The Installation of Submarine Power Cables under UNCLOS: Legal and Policy Issues,” *German Yearbook of International Law* 56 (2013): 107–48.

³ Edward J. Malecki and Hu Wei, “A Wired World: The Evolving Geography of Submarine Cables and the Shift to Asia,” *Annals of the Association of American Geographers* 99, no. 2 (2009): 360–82, <https://doi.org/>; Tara Davenport, “Submarine Communications Cables and Science: A New Frontier in Ocean Governance?,” in *Science Technology, and New Challenges to Ocean Law*, ed. Harry N. Scheiber and Moon-Sang Kwon (Leiden: Brill, 2015), 209–52; and Emily Waltz, “Offshore Wind May Power the Future,” *Scientific American*, 20 October 2008, <https://www.scientificamerican.com/>.

advanced technologies, has gained prominence. Historically, the control of information and communication systems has been leveraged for political and strategic gains, involving disinformation campaigns, propaganda, and other manipulative tactics to influence political landscapes and even topple governments. In the contemporary context, the widespread reach of ICT has amplified the capacity of malevolent actors and states to sway larger populations to serve their vested interests.⁴

The notion of hybrid warfare has gained substantial traction, particularly following Russia's invasion of Ukraine. Ongoing uncertainties surrounding projects like the Nord Stream and Nord Stream 2, involving multi-billion-dollar natural gas pipelines through the Baltic Sea, have fueled conspiracy theories regarding the vulnerability of undersea critical infrastructure. This infrastructure is seen as potential attack sites for malevolent actors seeking to exploit vulnerabilities in nation-states related to energy, power, and information.⁵

The Significance of Submarine Data Cables

In today's interconnected world, the Internet and e-communications rely heavily on submarine data cables. These undersea cables facilitate the transmission of vast amounts of data, Internet traffic, and voice across oceans and nations, serving as the backbone of the contemporary global landscape.⁶ The inception of long-distance undersea cable communication dates to the nineteenth century when the first undersea data cable, used for telegraphy, was laid in 1850. This copper-based telegraph wire connected the United Kingdom and France beneath the English Channel. Subsequently, the first successful transatlantic cable was established in 1866, marking significant milestones in long-distance communication technology.⁷

The evolution of undersea cables has seen them become more advanced and extensive, spanning over a million kilometers across the ocean floor, linking continents, islands, and nation-states. In today's world characterized by "complex interdependence," submarine data cables have emerged as one of the most critical infrastructures, raising concerns about potential anthropogenic and natural threats that could disrupt communication networks, thereby impacting economies ranging from single states to entire continents. Consequently, there is a pressing need for

⁴ Ofer Fridman, Vitaly Kabernik, James C. Pearce, eds. *Hybrid Conflicts and Information Warfare: New Labels, Old Politics* (Boulder, CO: Lynne Rienner, 2018), 1.

⁵ "White House Says Blog Post on Nord Stream Explosion 'Utterly False,'" *Reuters*, 8 February 2023, <https://www.reuters.com/>.

⁶ Nicole Starosielski, *The Undersea Network* (Durham, NC: Duke University Press, 2015), 1–25.

⁷ Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 2021).

a comprehensive evaluation of the governance architecture governing the laying, protection, and security of these vital undersea data cable infrastructures.

Authoritarian Regimes and Control over Data Cables

Information and communication pathways are pivotal for the global community, often described as a “powerful tool, for liberation or repression, depending on who controls it.”⁸ In this context, it is imperative to examine the role of authoritarian regimes such as the People’s Republic of China (PRC) in exerting overarching control over the undersea data cable industry. This control is pursued through a civil-military fusion strategy, where the civil sector collaborates with the military sector to realize the Chinese dream of “the great rejuvenation of the Chinese nation” by 2049.

The PRC’s Digital Silk Road (DSR), announced in 2015 as part of its Belt and Road Initiative (BRI), underscores the clear linkage between digital connectivity and Beijing’s geopolitical and geostrategic ambitions of establishing a Sino-centric global order. To this end, the PRC is making substantial investments through both private and state-owned firms in the submarine data cable sector and its supporting infrastructure. The civil-military fusion approach facilitates the global expansion of these companies while aligning them with China’s grand geopolitical objectives. A pertinent example discussed in this paper is the planned Pakistan and East Africa Connecting Europe (PEACE) submarine data cable project by the PRC, which holds the potential to become a significant geopolitical flashpoint in the WIO region. The strategic advantage gained by the PRC in the region could have far-reaching implications for regional security architecture, a matter of critical concern for India and its interests.

Securitization of Submarine Data Cables

India and the world rely heavily on the intricate network of submarine cables crisscrossing the seabed. These cables serve as strategic communication chokepoints in the global information highway, rendering them critical assets for global security. Responsible for carrying nearly 97 percent of worldwide Internet traffic, these submarine cables represent a tangible form of transnational connectivity that remains inadequately explored within the global geopolitical and geosecurity discourse.⁹ The absence of a clearly defined international governance framework has

⁸ Hillman, *The Digital Silk Road*.

⁹ James Dean et al., *Threats to Undersea Cable Communications* (Washington, DC: Public-Private Analytic Exchange Program, 28 September 2017), <https://www.hsdl.org/>.

given rise to security concerns, rendering these cables susceptible to sabotage and espionage, both in times of peace and war. These cables can grant nation-states a significant geopolitical and geostrategic advantage in international affairs. As of 2023, approximately 529 cable systems (totaling approximately 1.3 million kilometers in length) and 1,444 landing stations are operational or under construction.¹⁰

Submarine cables stand out as the swiftest, most cost-effective, and reliable means for global data transmission. In an era where the world's reliance on digital technology encompasses civilian communication, commerce, agriculture, healthcare, military logistics, and financial transactions, these subaquatic cables encased in steel and plastic have become indispensable to national security. Any disruption to these cables could paralyze the affected region and push the world to the brink of a 'new great depression.'¹¹ An illustrative incident occurred in January 2022 when a volcanic eruption severed the sole fiber-optic cable connecting Tonga to the rest of the world—the Tonga Cable to Fiji. This event left Tonga in a state of information isolation, resulting in severe economic losses and hindering the prompt and effective coordination of international humanitarian assistance. This episode underscored the heightened security imperative surrounding these cables, which are pivotal for global connectivity.¹²

Viewed from the perspective that nearly all governments worldwide utilize these cables to facilitate external and domestic communication, the significance of submarine cables in diplomacy, military communications, and trade and commerce cannot be overstated. These cables facilitate the transmission of transactions worth up to 10 trillion USD per day, primarily through private entities, as government-owned satellite usage for classified data remains limited. Consequently, the heavy reliance on these critical infrastructure components by government and military agencies can have catastrophic repercussions on a state's security and its ability to respond to emerging threats. A case in point is the 2008 incident when a submarine cable between Egypt and Italy ruptured, resulting in a substantial decline in US unmanned drone flights to Iraq.¹³ Thus, the question of ownership, construction, operation, and control of these critical infrastructures has become more relevant than ever before.

¹⁰ "Submarine Cable Frequently Asked Questions," *TeleGeography*, 2023, <https://www2.telegeography.com/>.

¹¹ James Rickards, *The New Great Depression: Winners and Losers in a Post-Pandemic World* (New York: Portfolio/Penguin, 2021).

¹² Winston Qiu, "Tonga Cables Cut after Volcanic Eruption, at Least Four Weeks to Restore," *Submarine Cable Networks*, 19 January 2022, <https://www.submarinenetworks.com/>.

¹³ Michael Sechrist, "Cyberspace in Deep Water: Protecting Undersea Communications Cables by Creating an International Public-Private Partnership" (policy analysis exercise, Harvard Kennedy School of Government, 23 March 2010), <https://www.belfercenter.org/>.

The private sector holds a monopoly over the planning, production, deployment, and maintenance of these submarine cables. Presently, SubCom of the United States of America, Alcatel Submarine Network of France, NEC of Japan, and Huawei Marine Networks of China rank as the four largest suppliers, owners, and builders of submarine cables globally.¹⁴ China's share in the global submarine cable sector rose to 11.4 percent in 2019, with China now aiming to expand its share to 20 percent between 2025 and 2030.¹⁵

Recently, the critical nature of the submarine cable communication network has come to the fore in the security considerations of the Western strategic community. Concerns have arisen about Russia potentially leveraging these undersea cables to disrupt their communication linkages with the world, thereby crippling their economies and other facets of daily life in retaliation for their support to Ukraine in the ongoing conflict. Heightened concerns stem from increased Russian submarine activity in proximity to these undersea cables. Britain's Admiral Tony Radakin remarked, "Undersea cables that transmit Internet data are 'the world's real information system,' and added that any attempt to damage them could be considered an 'act of war.'"¹⁶ Consequently, the possibility of submarine cable sabotage in times of peace or conflict has accentuated vulnerabilities, risk factors, and disruption indicators within the global submarine cable network and supporting infrastructure, including the undersea cables in the WIO.

Against the backdrop of the escalating technological rivalry between India and China, especially in the realms of espionage and data acquisition, it becomes imperative to acknowledge the pervasive role of submarine cables in these intensifying geopolitical frictions. China's DSR strategy emerges as a potent instrument that could be wielded to potentially disrupt, sabotage, or clandestinely gather intelligence from undersea cables. These cables serve as the linchpin of global communication networks and are critical to the strategic interests of both nations. Deliberate manipulation or compromise of undersea cables could provide China with a distinct geopolitical advantage in the ongoing competition or future conflicts with India in the region.

¹⁴ Colin Wall and Pierre Morcos, "Invisible and Vital: Undersea Cables and Transatlantic Security," Center for Strategic and International Studies, 11 June 2021, <https://www.csis.org/>.

¹⁵ Helene Fouquet, "China's 7,500-Mile Undersea Cable to Europe Fuels Internet Feud," *Bloomberg*, 4 March 2021, <https://www.bloomberg.com/>.

¹⁶ PA Media, "UK Military Chief Warns of Russian Threat to Vital Undersea Cables," *The Guardian*, 8 January 8, 2022, <https://www.theguardian.com/>.

Digital Silk Road: China's Underwater Expansion and Digital Warfare Strategy

Announced in 2015 as a digital component of the BRI, the PRC's DSR plan aims to construct a Sino-centric digital infrastructure. Its objectives include exporting Beijing's digital capabilities, promoting Chinese technology businesses, and gaining access to vast data repositories. The PRC envisions the DSR expanding its digital influence across the wider Indo-Pacific region by investing in critical information and digital infrastructure, including undersea cables, fiber-optic networks, fifth-generation (5G) networks, and data centers abroad.¹⁷

Consequently, there has been a notable increase in Beijing's engagement with African, Latin American, and West Asian states, particularly in digital infrastructure development. This engagement presents significant opportunities. As a subset of the BRI, the DSR strategically supports the PRC's aspiration for national rejuvenation by 2049. It achieves this through financing, constructing, and developing infrastructure in Indo-Pacific countries. A prime example is the extensive involvement of Chinese multinational corporation (MNC) Huawei in the development of critical information infrastructure across many African nations, with particular attention drawn to the "Safe Cities" program. Analysts have raised concerns, suspecting Beijing of employing its MNCs as state agents to surveil and exert authoritarian control over digital information flow to serve the Chinese Communist Party's (CCP) interests in resource-rich African regions.¹⁸

More than 150 countries have signed cooperation agreements related to China's BRI.¹⁹ Beijing intends to employ the DSR as a potent instrument to advance its expansionist policies and employ economic coercion through a skillfully designed civil-military fusion strategy.

China continues to enhance its unconventional capabilities to gain an advantage in the digital warfare landscape. The CCP invests in modernizing the People's Liberation Army (PLA) Navy, enabling it to expand naval assets underwater. This expansion is aimed at effectively disrupting adversary communication lines in digital warfare. China's preparations are oriented toward asymmetric conflict, focusing on operating in "gray zones" rather than engaging in full-scale

¹⁷ *Military and Security Developments Involving the People's Republic of China* (Washington, DC: Office of the Secretary of Defense, 2020), <https://media.defense.gov/>.

¹⁸ Bulelani Jili, "A Technological Fix: The Adoption of Chinese Public Security Systems," *Georgetown Journal of International Affairs*, 20 January 2023, <https://gjia.georgetown.edu/>.

¹⁹ Xue Gong, "The Belt and Road Initiative Is Still China's 'Gala' but Without as Much Luster," Carnegie Endowment for International Peace, 3 March 2023, <https://carnegieendowment.org/>.

wars.²⁰ This digital warfare strategy promises substantial results with minimal investment in resources.

In this context, Beijing's DSR seeks to establish a Sino-centric global digital order by expanding and exporting Chinese technology through state-controlled and private corporations.²¹ This strategy grants the PRC access to extensive data repositories. In 1999, the PRC introduced its 'Go Out' or 'Going Global' strategy, incentivizing state-owned and private corporations to invest and expand globally.²² Beijing provided incentives and subsidized loans to technology firms to expand to strategic regions worldwide.²³ Additionally, China enacted multiple laws mandating Chinese firms to "support, assist, and cooperate in government's intelligence and national security efforts."²⁴

One such law is the National Intelligence Law of 2017, obligating all organizations and citizens to cooperate with state intelligence work and maintain the secrecy of national intelligence work. This grants the CCP extraordinary powers to engage in sabotage, espionage, hacking, and surveillance of an adversary's communication networks, enabling the collection of sensitive economic, diplomatic, and military information required to pursue its strategic goals.²⁵ This threat to US communication networks was acknowledged in the 2019 *Worldwide Threat Assessment* report, where the Director of National Intelligence warned that "China presents a persistent cyber-espionage threat and a growing attack threat to our core military and critical infrastructure systems."²⁶

With the planned PEACE submarine cable becoming operational, China's expansion in undersea infrastructure and digital authoritarianism will receive a significant boost. The CCP harnesses cutting-edge communications technology to strengthen its control domestically and expand its influence abroad. The PEACE

²⁰ Peter Layton, "Bringing the Grey Zone into Focus," *The Interpreter*, 22 July 2021, <https://www.lowyinstitute.org/>.

²¹ *Military and Security Developments Involving the People's Republic of China* (2020).

²² Nargiza Salidjanova, *Going Out: An Overview of China's Outward Foreign Direct Investment* (Washington, DC: U.S.–China Economic & Security Review Commission, 30 March 2011), <https://www.uscc.gov/>.

²³ Hongying Wang, "A Deeper Look at China's "Going Out" Policy," Centre for International Governance Innovation, 8 March 2016, <https://www.cigionline.org/>; and Salidjanova, *Going Out*.

²⁴ National Intelligence Law of the People's Republic, Art. 7 (adopted 27 June 2017), <http://cs.brown.edu/>. Also, see other relevant Chinese laws obligating citizens and organizations to assist in "national security" efforts, including laws on Counterespionage (2014), National Security (2015), Counterterrorism (2015), and Cybersecurity (2016).

²⁵ 4 National Intelligence Law of the People's Republic, Art. 7.

²⁶ Statement of Daniel R. Coats, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record to the Select Committee on Intelligence, 116th Cong. 5, Sess. 1 (29 January 2019), <https://www.dni.gov/>.

cable, privately owned and invested in by Peace Cable International Network Co., Limited (a subsidiary of China's HENGTONG Group) and supplied by HMN Tech (formerly Huawei Marine Networks), will grant China a vital advantage in the region.²⁷ The project comprises three segments. Initially, a submarine cable will extend from Pakistan to France, passing through the Red Sea and Suez Canal, ultimately landing in France. Another branch of the PEACE cable will traverse Eastern Africa, connecting Kenya and Seychelles, and continue to the Maldives before finally reaching Singapore. The third and final leg of the PEACE cable will stretch toward South Africa, providing connectivity to the Southern African Development Community (SADC), East Africa, West Asia, and Europe, thus expanding the Chinese digital footprint. This strategic expansion positions China to assert itself both geopolitically and geoeconomically, potentially challenging the dominance of the United States and India in the region.

China currently possesses key infrastructure assets in areas of significant geopolitical importance, including the port of Gwadar, Pakistan, operated by China Overseas Ports Holding Company; Djibouti (China's first overseas military base); and Egypt (Beijing's largest trading partner in the region). These assets are strategically vital to Beijing's geopolitical ambitions, as they facilitate its trade and energy imports through key chokepoints adjoining these states. Thus, China and Huawei, the project implementer, have strategically selected nations of significant geostrategic importance as intermediary locations to further their objectives and strategic activities.

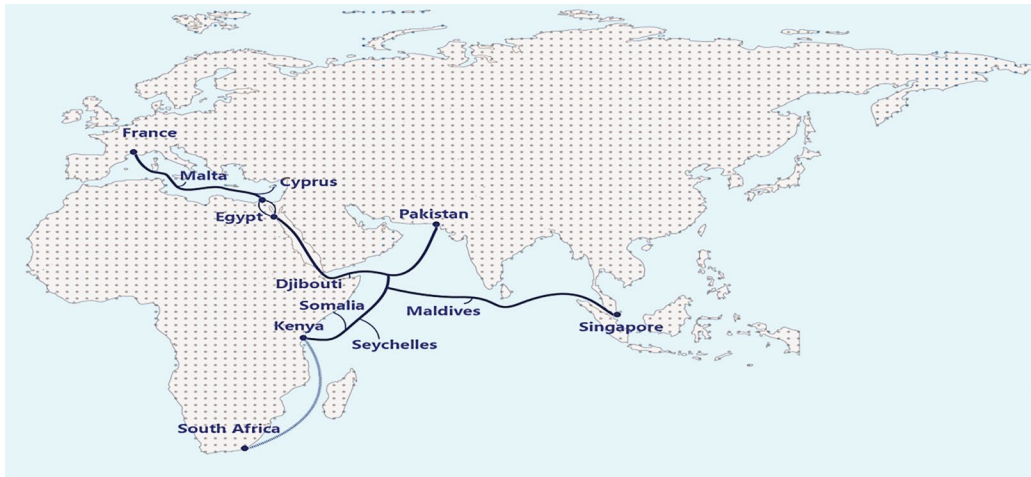


Fig 1. PEACE: A 15,000-km-long network connecting Asia, Africa, and Europe. (Source: Peace Cable International Network Co., Limited <http://www.peacecable.net/>.)

²⁷ "PEACE," *Submarine Cable Networks* (website), n.d., <https://www.submarinenetworks.com/>.

With the PEACE cable, China establishes a permanent presence in the strategic chokepoints of these critical infrastructures. Landing stations in Pakistan and Djibouti provide the PLA Navy with a strategic advantage, enabling permanent stationing in the WIO region and facilitating the collection of strategic information for both above and undersea operations in these key chokepoints. Chinese investments in digital infrastructure, fiber-optic cables, business partnerships, and technical expertise within these pivotal nations will amplify Beijing's influence as these economies transition to digital platforms. China's growing economic and soft-power influence, driven by infrastructure and digital initiatives, has the potential to displace India from its traditionally dominant position in its extended maritime neighborhood. As Beijing shifts its focus to the WIO and the wider Indo-Pacific, countries like Pakistan, Djibouti, and Egypt, with their significant digital intersections and vital water passages, may increasingly align with China's sphere of influence. Submarine cables landing in mainland China or facilities financed by China's BRI loans grant the PRC the leverage to conduct extensive geopolitical propaganda campaigns, aiming to deny opponents the strategic advantage of space and technology in ongoing great-power competition.

UNDERSEA CABLE CHOKE POINTS AFFECTING ASIA & MIDDLE EAST

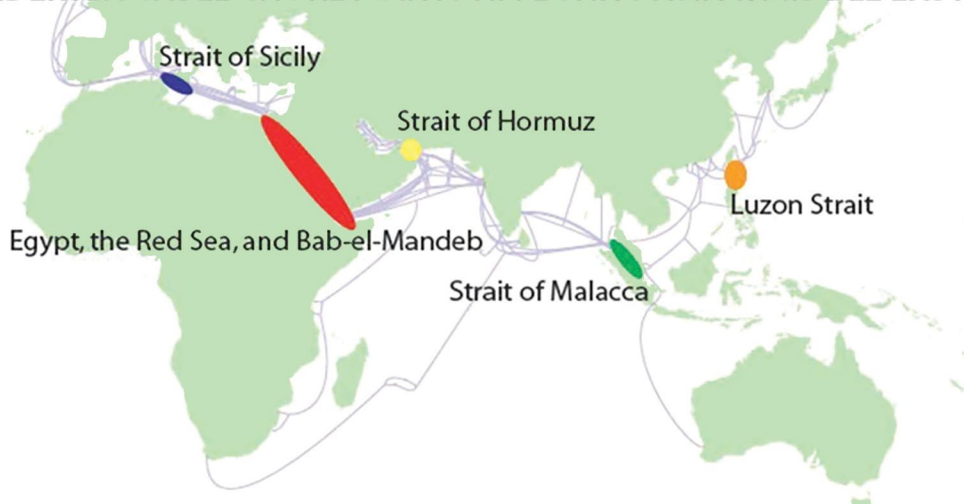


Figure 2. Undersea cable chokepoints affecting Asia and the Middle East. (Source: "Arctic Submarine Fiber-optic Cable Line Polar Express," *Morsviazputnik* (website), 2020, <https://www.marsat.ru/>.)

The Security Challenge: Sabotage and Espionage

Submarine cables represent critical infrastructure susceptible to sabotage and espionage, including physical damage. Any disruption of these cables could have

devastating global repercussions. Sabotaging these cables can be viewed as a strategic maneuver to weaken an adversary prior to the outbreak of kinetic warfare.²⁸ States or state-sponsored nonstate actors often employ specially equipped submarines and techniques to tap or completely sever undersea cables, as exemplified in 2013 when three individuals equipped with specialized scuba gear and fishing boats attempted to cut the SEA-ME-WE 4 undersea cable. This incident disrupted communication traffic between Europe and Egypt, underscoring the vulnerability of these vital assets.²⁹

Another critical infrastructure at risk of sabotage is the cable landing stations, where undersea cables connect to terrestrial digital communication networks. The convergence of multiple cables at these stations makes them prime targets during conflicts. Additionally, natural threats like shark attacks, earthquakes, and tsunamis pose a risk of disruption. However, what concerns the strategic community most is the deliberate threat to these crucial assets. Chinese fishing fleets, under the guise of human error, could intentionally damage these cables, or specialized units of the PLA Navy might undertake missions to disrupt communication flow.

Recent events have underscored the potential for undersea cables to become embroiled in conflicts involving China and Taiwan. In February 2023, Chinese maritime vessels severed two communication cables linking Taiwan with its Matsu islands, causing Internet connectivity disruptions for the island's residents. The "unintended" targeting of these cables near China's coast could be interpreted as a calculated maneuver to demonstrate China's capability to disrupt communication and potentially isolate Taiwan.³⁰ These incidents highlight the significance of undersea cables as tools for leveraging power in modern conflicts.

In contrast, espionage does not necessarily entail damage or disruption to undersea cables but is executed covertly to gain access to data flowing through these cables, either underwater or at designated landing or data centers. This requires specialized training and techniques. The PLA's Science and Engineering University provides tailored training in advanced digital warfare and research related to defense technology and military equipment.³¹ China is rapidly closing the gap with the US and Russia in this domain. Russia, for instance, possesses the AGS, a small

²⁸ Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, no. 2 (2014): 181–92, <https://direct.mit.edu/>.

²⁹ Charles Arthur, "Undersea Internet Cables off Egypt Disrupted as Navy Arrests Three," *The Guardian*, 28 March 2013, <https://www.theguardian.com/>.

³⁰ Wen Lii, "After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience," *The Diplomat*, 15 April 2023, <https://thediplomat.com/>.

³¹ Thomas J. Bickford, "Professional Military Education in the Chinese People's Liberation Army: A Preliminary Assessment of Problems and Prospects," in *A Poverty of Riches: New Challenges and Opportunities in*

nuclear-powered minisubmarine capable of tapping fiber-optic cables in challenging underwater environments.³² The United States has also conducted cable-tapping operations, notably during the Cold War when the submarine USS *Halibut* intercepted sensitive information from a military cable passing through the Sea of Okhotsk to the Kamchatka Peninsula in the eastern Soviet Union. This operation, codenamed Ivy Bells, continued for a decade and utilized three specially modified submarines.³³ The ability to tap and gather intelligence provides significant advantages to a nation's military. Tactics of sabotage and espionage can be employed simultaneously, as demonstrated by Britain during World War I when it severed most of Germany's undersea telegraph networks, leaving one cable intact, which was subsequently tapped to gather vital intelligence during the war.³⁴

The DSR is envisioned as a response to unconventional warfare, providing the PLA with command and control over the world's strategic communication gateways. Investments in these infrastructures aim to furnish the PRC with intelligence, military battlefield information, and geopolitical advantages far beyond its strike zones. The digital database enhances the PLA's operational flexibility and responsiveness in both conventional and unconventional warfare scenarios. The PLA regards digital warfare as an integral component of modern warfare, with an emphasis on "suppressing, degrading, disrupting, or deceiving enemy electronic equipment."³⁵ The US Department of Defense 2020 *Military and Security Developments Involving the People's Republic of China* clearly states that:

China has publicly identified cyberspace as a critical domain for national security and declared its intent to expedite the development of its cyber forces. The PRC presents significant, persistent cyber espionage and attack threats to military and critical infrastructure systems. China seeks to create disruptive and destructive effects—from denial-of-service attacks to physical disruptions of critical infrastructure—to shape decision-making and disrupt military operations in the initial stages of a conflict by targeting and exploiting perceived weaknesses of militarily superior adversaries. . . . Authoritative PLA sources call for the coordinated employment of space,

PLA Research, ed. James C. Mulvenon and Andrew N. D. Yang (Santa Monica, CA: RAND, 2003), 17, <https://www.rand.org/>.

³² H I Sutton, "How Russian Spy Submarines Can Interfere with Undersea Internet Cables," *Forbes*, 19 August 2020, <https://www.forbes.com/>.

³³ Sherry Sontag, Christopher Drew, and Annette Lawrence Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage* (New York: Public Affairs, 2016).

³⁴ Garrett Hinck, "Cutting the Cord: The Legal Regime Protecting Undersea Cables," *Lawfare* (blog), 21 November 2017, <https://www.lawfaremedia.org/>.

³⁵ *Military and Security Developments Involving the People's Republic of China* (2020).

cyber, and electronic warfare (EW) as strategic weapons to “paralyze the enemy’s operational system of systems” and “sabotage the enemy’s war command system of systems” early in a conflict. Increasingly, the PLA considers cyber capabilities a critical component in its overall integrated strategic deterrence posture, alongside space and nuclear deterrence.³⁶

Strategic Response and India’s Options

This article considers a matrix of potential strategic responses, taking into account the implications of the DSR on the geopolitical and geosecurity landscape in India’s extended maritime neighborhood. The absence of a singular or coordinated strategy for governing and securing submarine cables demands immediate attention. India possesses unrivaled demographic, economic, and geographical advantages, positioning New Delhi to emerge as a prominent global player in submarine cable networks. However, capitalizing on this substantial potential necessitates the Indian government’s establishment of policies and regulations that foster investment, aligning with its rapidly growing digital economy.

Assuming the pivotal role of a global and regional hub for submarine data cable networks, India can serve as a strategic countermeasure to China’s ambitions and enhance its digital prowess on the global stage. To achieve comprehensive and holistic security for undersea data cable systems, a combination of operational strategies and a robust safeguarding approach is imperative. This approach encompasses offshore patrolling, the establishment of cable protection zones, and the implementation of a well-defined security audit framework to counteract digital warfare threats.

As India rapidly grows its digital economy, it has compelling reasons to maintain vigilance regarding potential threats to undersea cables. Recognizing the vital importance of safeguarding its national prosperity and security, India should contemplate adopting innovative policy solutions reminiscent of the cable protection zones (CPZ) established by Australia and New Zealand. These CPZs would delineate restricted areas within India’s sovereign waters, where activities such as anchoring, bottom trawling, and specific types of fishing would face prohibitions to prevent cable damage. To ensure compliance, India could impose substantial fines on violators, mirroring the stringent framework outlined in Australia’s Telecommunications Act of 1997.³⁷ Furthermore, ships operating within these zones

³⁶ *Military and Security Developments Involving the People’s Republic of China* (2020), 83

³⁷ Telecommunications and Other Legislation Amendment (Protection of Submarine Cables and Other Measures) Act 2005. <https://www.legislation.gov.au/>.

should be mandated to transmit their positions to the Indian Coast Guard for continuous monitoring, utilizing coastal radar, surveillance aircraft, unmanned aerial vehicles, and surface patrols.

Steps taken, such as the creation of the tri-service Cyber Defense Agency in 2018 and the Telecom Regulatory Authority of India (TRAI) recommendations on Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India, demonstrate India's commitment in the right direction.³⁸ The recent TRAI legislation, which proposes designating undersea cables as critical information infrastructure eligible for protection by the National Critical Information Infrastructure Protection Centre (NCIIPC), enhances their security and shields against potential cyberthreats, strengthening their safeguarding. Nevertheless, addressing this transnational security challenge calls for a more comprehensive response.

Like-minded nation-states should collaborate to provide a democratic digital network alternative to China's autocratic offerings. Initiatives by the Quad group of countries, including India, Japan, Australia, and the United States, alongside other like-minded powers such as the European Union, should aim to challenge China's dominant position in this technological domain. Positive steps in this direction are already evident, with efforts to develop regulatory frameworks for the subsea cable market and the formation of the Working Group on Critical and Emerging Technologies showcasing intent to collaborate in this strategic field.³⁹

The Quad Partnership for Cable Connectivity and Resilience, with a focus on enhancing Indo-Pacific cable systems through the expertise of Quad nations, prioritizes regional infrastructure and represents a welcome decision. Its aim is to unite public and private sector stakeholders to rectify infrastructure deficiencies and synchronize future advancements, a mission that will assume a pivotal role in forging a democratic and open communication route for the Indo-Pacific region and beyond, thereby ensuring heightened connectivity and resilience. Initiatives like Australia's Indo-Pacific Cable Connectivity and Resilience Program and the United States' offer of assistance through the CABLES program are likely to yield positive results in containing China's expansionism in the digital domain.⁴⁰

To ensure the robust protection and sustained growth of undersea cable infrastructure in the WIO and beyond, New Delhi must harness India's rapidly expand-

³⁸ "TRAI releases recommendations on 'Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India'" (press release, Ministry of Communications [India], 20 June 2023), <https://pib.gov.in/>.

³⁹ Elizabeth Roche, "Quad Can Pool Resources to Prevent China from Dominating Global Tech," *Live Mint*, 28 June 2021, <https://www.livemint.com/>. Also see, "Quad Summit" (fact sheet, The White House, 12 March 2021), <https://www.whitehouse.gov/>.

⁴⁰ "Quad Leaders' Summit Fact Sheet" (fact sheet, The White House, 20 May 2023), <https://www.whitehouse.gov/>.

ing digital economy, its strategic location as a global connectivity hub, its abundant technical expertise in the tech industry, its rising global influence, and ongoing efforts to expand connectivity. In this context, the launch of the transcontinental and transoceanic India–Middle East–Europe Economic Corridor (IMEC) during the recently concluded G-20 summit in New Delhi represents a bold geo-economic initiative of unprecedented scale since China unveiled its BRI in 2013.⁴¹ The IMEC unites capable partner nations to pool resources, reshape supply chains, production networks, and spheres of influence under the Partnership for Global Infrastructure and Investment (PGII) initiative, reducing overreliance on China in global trade and critical infrastructure. The corridor encompasses a comprehensive scope, including a rail link, an electricity cable, a hydrogen pipeline, and a high-speed data cable. Unlike the opaque and nontransparent nature of the BRI, the IMEC prioritizes viability and draws funding from multiple sources, particularly through public-private partnerships, fostering a technological ecosystem characterized by resilience, integrity, openness, trust, and security, reinforcing democratic principles and human rights. Through the IMEC, India leverages its strategic position to collaborate with friendly foreign nations, countering China’s influence and offering a democratic alternative to the global community. Together, like-minded countries organize and mobilize to ensure technologies align with, rather than undermine, democratic principles, institutions, and societies.

In the context of undersea cables spanning diverse territorial waters and subject to varying national policies and regulations, the release of the “ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables” in 2019 serves as a notable precedent.⁴² Drawing inspiration from the ASEAN initiative, India can take a leadership role in advocating for the development of a similar guideline within the Indian Ocean Rim Association (IORA), streamlining and simplifying the permit application process for cable repair. Furthermore, by leveraging the collaborative potential of the Indian Ocean Naval Symposium (IONS), India can foster cooperative mechanisms aimed at enhancing the safety and security of submarine cables. The region’s multilateral maritime mechanisms, exemplified by IORA, hold promise in addressing nontraditional security threats, especially in light of recent efforts to address maritime security concerns. IONS, serving as a forum for naval professionals from 35 member states, provides a strategic platform

⁴¹ “Partnership for Global Infrastructure and Investment (PGII) & India-Middle East-Europe Economic Corridor (IMEC)” (press release, Ministry of External Affairs [India], 9 September 2023), <https://www.mea.gov.in/>.

⁴² “ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables,” ASEAN, n.d., <https://asean.org/>.

for knowledge exchange and consensus-building on maritime security matters in the Indian Ocean, making it an ideal avenue for collaborative submarine cable protection initiatives.

Additional strategies should involve restricting the transmission of sensitive and critical data through privately owned submarine cables. Moreover, prioritizing national capacity enhancement and investing in military modernization for securing these vital undersea cable networks must take precedence. Regular risk assessments and monitoring of these cable projects should be integrated into states' defensive and offensive strategies. Hence, it is imperative for India to expedite its efforts in developing and integrating autonomous unmanned systems, particularly unmanned underwater vehicles (UUV), into its naval operations. The delayed construction and procurement of high endurance autonomous underwater vehicles (HEAUV) underscore the urgent need for enhancing undersea domain awareness capabilities. While domestic production is desirable, immediate reliance on UUV imports is critical to bridge the capacity gap. Collaborative endeavors involving private companies, research and development projects, and an inclusive approach that engages all stakeholders will be pivotal in accelerating UUV technology advancement, crucial for underwater warfare. The approved flagship project for extra-large unmanned underwater vehicles (XLUUV) should be vigorously pursued, with the prototype slated for completion by 2025.⁴³ These XLUUVs, designed for intelligence, surveillance, and reconnaissance, antisubmarine, surface, and mine warfare, will significantly enhance India's underwater domain awareness (UDA) capabilities, aligning with the evolving security landscape of naval operations in the Indian Ocean region.

Given that a significant majority of these cables are owned, operated, and managed by private firms, ensuring the private sector's commitment to national security becomes an essential aspect of policy planning. Encouraging public-private partnership models in this sector can mitigate risks associated with sabotage and espionage. Equally important is the development of a contingency plan to address disruptions promptly.

Lastly, India should engage with the international community and unite like-minded states to establish a comprehensive international legal framework for securing these critical infrastructures.

⁴³ Government of India, "Invitation for Expression of Interest (EOI): Indigenous Development of High Endurance Autonomous Underwater Vehicle—Anti-Submarine Warfare Project HEAUY-ASW," Make in India Defence, 24 March 2023, <https://www.makeinindiadefence.gov.in/>.

Conclusion

As we delve into the depths of the world's oceans, an inconspicuous yet significant battle for global supremacy is underway. China's digital warfare strategy is crystallizing through initiatives like the PEACE cable and its establishment of undersea bases for submarine cables in the South China Sea and the East China Sea. The Western and Indian strategic communities are acutely aware of China's growing capacity and capability to extend its digital dominance across the globe.

The global community's increasing reliance on China's technologies has far-reaching implications for geopolitics, economies, and global security. China's planned PEACE cables are forging deep connections into the East African and West Asian regions, posing threats to national, regional, and global security.

Given the constraints India faces, it becomes imperative to embark on a coordinated effort to develop critical infrastructure that can match China's potential. The DSR, designed to facilitate China's ascent to superpower status with unconventional strategies, demands counterstrategies to curtail China's rise.

In the depths of the undersea world, the stage is set for a battle of digital supremacy. How nations respond to this challenge will shape the future of global information networks and the balance of power in the digital age. The undersea cables, often hidden from view but fundamental to our interconnected world, have become the battleground where the struggle for dominance plays out. 🌐

Raghvendra Kumar

Mr. Kumar (ORCID ID: 0000-0002-6872-3681) is an independent researcher and analyst specializing in Indian Ocean geopolitics and maritime affairs. He has recently submitted his doctoral thesis, "China's Engagement with Western Indian Ocean Island States of Africa: Implications for India," to the Department of African Studies at the University of Delhi, India. Previously he worked as an associate fellow at the Africa's Maritime Geostратегies (AMG) Cluster, of the esteemed National Maritime Foundation (NMF), Delhi, enhancing his expertise in maritime geostратегies. Prior to his tenure at the NMF, Mr. Kumar taught undergraduate students at the Department of Political Science, Maharaja Agrasen College, University of Delhi. His areas of interest include but are not limited to Africa in the Indian Ocean, India and China in Indian Ocean geopolitics, maritime security studies, and nontraditional security challenges. He can be reached at raghvendrakumar2007@gmail.com.

Acknowledgement: The author would like to express sincere gratitude to Prof. Christian Bueger for his invaluable feedback and insightful remarks on this article. His expertise and guidance have greatly enriched the quality of this work.

Disclaimer

The views and opinions expressed or implied in JIPA are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Department of the Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government or their international equivalents.