What are the specific geopolitical consequences of China's undersea data center deployments?

April 19, 2026 | SnugLab Research | readme.snuglab.com

Executive Summary

China's undersea data center deployments create significant geopolitical consequences, primarily by establishing strategic vulnerabilities through pervasive surveillance capabilities and potential network chokepoints, while simultaneously offering substantial operational efficiencies. These deployments, integrated within the Digital Silk Road, enable Beijing to monitor and potentially manipulate global information flows, exert coercive influence, and make vital connectivity targets for "gray-zone" interference, particularly in contested maritime zones [12, 13]. Concurrently, the technology offers up to 90% energy savings for cooling and enhances hardware reliability, supporting the energy demands of AI while reducing carbon emissions [4].

Key Findings

Surveillance and Information Control

China's undersea data center deployments facilitate surveillance and information control through a strategy of "weaponized interdependence" [5, 6]. This includes the "Panopticon Effect," which allows for strategic intelligence gathering as global data flows through Chinese-controlled infrastructure, and the "Chokepoint Effect," enabling the disruption of network access during crises [5, 6]. Surveillance is further supported by the "Great Underwater Wall," a network of sensors and unmanned underwater vehicles (UUVs) used to observe maritime activity [5, 6]. Software-Defined Networking (SDN) also allows for data rerouting, which could facilitate interception [5, 6]. These infrastructures are vulnerable to "gray-zone" threats, including potential cable sabotage in critical regions like the Taiwan Strait and South China Sea [2, 5, 6, 11].

While these risks are significant, the shift toward distributed edge computing and distributed networks may enhance the resilience and geographical dispersion of the digital ecosystem [5, 6].

Chokepoint Effect and Supply Chain Dominance

China's control over the subsea cable supply chain creates a "Chokepoint Effect," allowing for the disruption or denial of network access to adversaries during crises [5, 6]. This poses a substantial threat to global financial networks, as 95% to 99% of all international and intercontinental internet traffic relies on submarine cables [5, 6, 8]. This infrastructure is critical for financial transactions, including the SWIFT network, which processes approximately US$10 trillion daily [1, 5, 6].

China's "Digital Silk Road" initiative aims to capture 60% of the global fiber-optic cable market [2, 5, 6]. As of 2025, Chinese companies, including YOFC, Hengtong, FiberHome, and Jiangsu Zhongtian Technology, controlled more than 35% of the global market [2]. HMN Technologies is also the world's fourth-largest and fastest-growing subsea cable builder [2]. This dominance is further reinforced by China's control over nearly 99% of the world's heavy rare earth element processing as of 2023, which is essential for the hardware used in subsea infrastructure [7]. As Jason Hsu noted, "For U.S. allies and partners, allowing China to dominate subsea cable construction and ownership in emerging markets would increase the risk that Beijing could conduct surveillance, intercept data, or deliberately disrupt networks" [2].

Gray-Zone Warfare and Cable Vulnerabilities

Submarine cable disruptions in the Taiwan Strait and South China Sea are attributed to both intentional "gray-zone" warfare tactics and accidental damage [1, 2, 5, 6, 11]. China employs "gray-zone" actions, which are intended to pressure opponents without triggering conventional war, to target cables in these regions [2, 5, 6, 11]. For instance, in early 2025, Taiwan experienced four submarine cable disruptions, including the severing of the Trans-Pacific Express cable by a vessel controlled by a Hong Kong company [2]. In February 2023, a Chinese fishing boat and a Chinese cargo vessel severed two cables connecting Taiwan's Matsu Islands to the mainland [2]. Despite these incidents, researchers acknowledge that these cables are inherently susceptible to accidental damage [1, 2, 5, 6, 11].

Strategic Dependencies and Operational Efficiency

The integration of undersea data centers (UDCs) with offshore renewable energy and heavy rare earth element processing creates a tension between significant operational

energy savings and critical geopolitical supply-chain vulnerabilities. UDCs offer substantial operational efficiency, with natural seawater cooling reducing energy consumption for cooling by up to 90% [4]. A project in Shanghai, for example, uses at least 30% less electricity than land-based centers and draws approximately 95% of its energy from offshore wind farms [4, 10]. As one report states, "It will serve clients such as China Telecom and a state-owned AI computing company, and is part of a broader government push to lower data centers' carbon footprint" [4].

However, this infrastructure is linked to strategic dependency due to China's control over nearly 99% of the world's heavy rare earth element processing as of 2023, which is crucial for the hardware and energy infrastructure required for AI [7].

Physical Sabotage and Environmental Concerns

Physical sabotage via UUVs and sensors represents a more direct threat to international maritime security compared to thermal pollution. This is a central component of China's "gray-zone" warfare [2, 5, 6, 11]. China's "Great Underwater Wall" surveillance network, comprising sensors and UUVs, monitors maritime activity and enables the "Chokepoint Effect" to disrupt network access during crises [5, 6]. Documented economic damage includes an estimated $1.69 billion monthly loss for Taiwan following cable disruptions [2]. UDCs are also vulnerable to destruction via sound waves delivered through underwater speaker systems, as "Researchers at the University of Florida and the University of Electro-Communications in Japan have also found that submarine data centers can be vulnerable to attacks using sound waves conducted through water" [4].

The risk of "thermal pollution" to environmental stability is debated. While some warn of potential harm to marine biodiversity from scaling UDCs during heat waves, assessments of Chinese test projects indicate that heat dissipation caused less than a one-degree temperature rise [4, 10]. Within China's geopolitical strategy, physical sabotage and surveillance are more directly linked to "weaponized interdependence" [5, 6].

Key Players and Market Share

Highlander is a leading developer of seawater-cooled undersea data center projects, such as the one in Shanghai [10]. In the broader subsea cable supply chain, Chinese companies including YOFC, Hengtong, FiberHome, and Jiangsu Zhongtian Technology

collectively controlled more than 35% of the global market as of 2025 [2]. HMN Technologies (formerly Huawei Marine Networks) is recognized as the world's fourth-largest and fastest-growing subsea cable builder [2]. China's "Digital Silk Road" initiative aims to achieve 60% of the global fiber-optic cable market [2, 5, 6].

Deployment Timelines and Alternative Projects

The provided research does not offer specific year-by-year deployment schedules or milestones for "Digital Silk Road" undersea infrastructure in the South China Sea through 2030. However, it indicates that by 2025, investment focus was projected to shift toward Southeast Asia, with fewer new projects directly connecting China to the rest of the world [9]. As one report noted, "No new projects will connect the country after 2025 as focus shifts to Southeast Asia" [9]. The South China Sea and Taiwan Strait are identified as key regions for geopolitical competition and potential "gray-zone" cable sabotage [2, 5, 6].

The research does not identify specific alternative infrastructure projects or consortiums, such as the Blue-Raman cable or Google/Meta-led projects, as direct geopolitical countermeasures to China's UDC expansion. Microsoft's Project Natick is mentioned as a "pioneering but now largely inactive or research-focused precedent" for underwater data centers [3, 4, 10].

Economic Vulnerabilities

The research does not identify specific "red line" thresholds or economic indicators that would trigger a coordinated international response to subsea dependencies. However, it details the scale of economic and data-driven vulnerabilities. Submarine cables carry between 95% and 99% of all international and intercontinental internet traffic [5, 6, 8], supporting the SWIFT network which processes approximately US$10 trillion daily [1, 5, 6]. The economic impact of disrupting digital communications in Taiwan is estimated at approximately $55 million per day, or $1.69 billion per month [2]. China's aim to capture 60% of the global fiber-optic cable market [2, 5, 6] and its control over nearly 99% of heavy rare earth element processing [7] further highlight these dependencies.

Implications

China's undersea data center deployments carry significant implications for global digital security, economic stability, and international relations. The "Chokepoint Effect" and "Panopticon Effect" enabled by China's growing control over subsea infrastructure and rare earth elements create a strategic vulnerability for nations reliant on these networks, particularly for critical financial transactions and intelligence gathering [2, 5, 6, 7]. The documented instances of "gray-zone" cable sabotage in contested regions like the Taiwan Strait demonstrate a willingness to disrupt connectivity, posing direct threats to regional stability and incurring substantial economic costs [2]. This strategic expansion, driven by the "Digital Silk Road," could lead to increased geopolitical tensions and a more fragmented global internet, where data flows are subject to state control and potential weaponization [2, 5, 6, 9].

Conversely, the operational efficiencies of undersea data centers, such as significant energy savings and enhanced hardware reliability, present a compelling case for their continued development, especially in supporting the massive energy demands of AI while pursuing carbon reduction goals [4, 10]. This creates a complex trade-off between the environmental and economic benefits of the technology and the geopolitical risks associated with its control and deployment by a single dominant power. The lack of identified alternative infrastructure projects as direct countermeasures suggests a potential gap in strategic responses to China's expanding influence in this critical domain.

Limitations and Caveats

The research provides a comprehensive overview of the geopolitical consequences but has certain limitations. Specific year-by-year deployment timelines and milestones for "Digital Silk Road" undersea infrastructure projects in the South China Sea through 2030 are not detailed. Furthermore, the research does not identify specific "red line" thresholds or economic indicators that would trigger a coordinated international response to subsea dependencies. There is also scientific disagreement regarding the long-term environmental impact of "thermal pollution" from UDCs on marine biodiversity, with some studies showing minimal temperature rise while others warn of potential harm at scale [4, 10]. The absence of identified direct geopolitical countermeasures to China's UDC expansion suggests an area for further investigation.

Sources

[1] [edu] Undersea Alliances Japan The U S And The Geopolitics Of Subm - jsis.washington.edu - https://jsis.washington.edu/news/undersea-alliances-japan-the-u-s-and-the-geopolitics-of-submarine-cable-security/

[2] Part Your World Us China Competition Under Sea Jason Hsu - hudson.org - https://www.hudson.org/technology/part-your-world-us-china-competition-under-sea-jason-hsu

[3] How Sustainable Is Chinas Wind Powered Subsea Data Centre - sustainabilitymag.com - https://sustainabilitymag.com/news/how-sustainable-is-chinas-wind-powered-subsea-data-centre

[4] Chinas New Underwater Data Centers Could Slash Power By Up T - sciencealert.com - https://www.sciencealert.com/chinas-new-underwater-data-centers-could-slash-power-by-up-to-90

[5] Wired For Power The Geopolitics Of Subsea Cables In The Sout - asianz.org.nz - https://www.asianz.org.nz/wired-for-power-the-geopolitics-of-subsea-cables-in-the-south-china-sea

[6] Wired For Power The Geopolitics Of Subsea Cables In The Sout - asiamediacentre.org.nz - https://www.asiamediacentre.org.nz/wired-for-power-the-geopolitics-of-subsea-cables-in-the-south-china-sea

[7] The Weakest Link Strategic Inputs In U S China Ai Competitio - ari.us - https://ari.us/policy-bytes/the-weakest-link-strategic-inputs-in-u-s-china-ai-competition/

[8] [news] 2025 Us Vs China Undersea Internet Cables - bloomberg.com - https://www.bloomberg.com/graphics/2025-us-vs-china-undersea-internet-cables/

[9] More Subsea Cables Bypass China As Sino U.S. Tensions Grow - asia.nikkei.com - https://asia.nikkei.com/spotlight/datawatch/more-subsea-cables-bypass-china-as-sino-u.s.-tensions-grow

[10] China Powers Ai Boom With Undersea Data Centers - scientificamerican.com - https://www.scientificamerican.com/article/china-powers-ai-boom-with-undersea-data-centers/

[11] [peer-reviewed] Article - sciencedirect.com - AUTHORS UNAVAILABLE - https://www.sciencedirect.com/science/article/pii/S0308597X25004282

[12] [wiki] Digital Silk Road - Wikipedia - https://en.wikipedia.org/wiki/Digital_Silk_Road

[13] China's Digital Silk Road Initiative | The Tech Arm of the Belt and ... - https://www.cfr.org/china-digital-silk-road/