Underwater Geopolitics

2 0 Save

The Chinese ship, the bulk carrier Yi Peng 3 (R) is anchored and being monitored by a Danish naval patrol vessels in the sea of Kattegat, near the City og Granaa in Jutland, Denmark, on Nov. 20, 2024. Denmark's navy said on Nov. 20, 2024 it was shadowing a Chinese cargo vessel in the Baltic Sea, a day after Finland and Sweden opened investigations into suspected sabotage of two severed undersea telecoms cables. Mikkel Berg Pedersen/Ritzau Scanpix/AFP via Getty Images

OPINION

By Carlo J.V. Caro
12/2/2024 Updated: 12/2/2024

Print

Commentary

How China's Control of Undersea Cables and Data Flows Reshapes Global Power

Cable Routing Protocols

The rapid construction of undersea cables has brought a hidden but crucial issue into focus: the manipulation of the protocols that control how data travels beneath the sea. These protocols determine the pathways internet data takes, influencing speed, costs, and even exposure to surveillance. Even small changes in these pathways can tilt the global balance of digital power. China's increasing role in this area demonstrates how technology can be used strategically to reshape geopolitics.

At the heart of this issue is a technology called Software-Defined Networking (SDN). SDN allows data traffic to be managed and optimized in real time, improving efficiency. But this same flexibility makes SDN vulnerable to misuse. Chinese tech companies like HMN Tech (formerly Huawei Marine Networks), ZTE, and China Unicom are leading the way in SDN development. China also holds sway in international organizations that set the rules for these technologies, such as the International Telecommunication Union (ITU) and the Institute of Electrical and Electronics Engineers (IEEE). This influence gives China a hand in shaping global standards and governance.

Africa illustrates how this influence plays out. Chinese investments in digital infrastructure across the continent are massive. For example, the PEACE (Pakistan and East Africa Connecting Europe) cable, which links East Africa to Europe, was designed to avoid Chinese territory. Yet, thanks to SDN technology, its traffic can still be redirected through Chinese-controlled points. This redirection could introduce delays of 20 to 30 milliseconds per hop—not much for casual browsing, but a serious issue for latency-sensitive activities like financial trading or encrypted communication.

In Southeast Asia, similar risks are evident. The Southeast Asia-Japan Cable (SJC), which connects Singapore to Japan, relies on several landing stations influenced by China. During a period of heightened tensions in the South China Sea, some data intended for Japan was mysteriously routed through Hainan Island, under Chinese jurisdiction. Such cases suggest technical routing decisions may sometimes have political motivations.

These examples are part of a broader strategy. By exploiting SDN, China can turn submarine cables into tools for surveillance and control. Data traffic from Africa or Southeast Asia destined for Europe could be secretly rerouted through Shanghai or Guangzhou, exposing it to China's advanced surveillance techniques like deep packet inspection. This threat extends to cloud computing, as major providers such as Amazon Web Services (AWS), Microsoft Azure, and Alibaba Cloud rely on undersea cables. With SDN, Chinese cloud providers—aligned with state interests—could redirect sensitive inter-cloud traffic, putting critical communications at risk.

Manipulating global data routes gives any actor significant geopolitical power. For instance, in a crisis, China could degrade or even sever internet connectivity for rival nations. In the Taiwan Strait, this could isolate Taiwan from global markets, disrupting financial transactions and trade. In Africa, where Huawei has built a significant portion of the continent's telecommunications infrastructure—reportedly constructing around 70 percent of 4G networks—there is concern that this reliance could create vulnerabilities. If political tensions were to arise, China could cause slowdowns or disruptions to reinforce dependence, making countries more vulnerable in political standoffs.

The numbers highlight the stakes. Submarine cables carry 99 percent of international data traffic—over 1.1 zettabytes annually. Significant portions of intra-Asia-Pacific data flows pass through key submarine cable landing stations, including Hong Kong, which is under Chinese jurisdiction. With Chinese firms increasingly involved in substantial global submarine cable projects—such as those undertaken by HMN

Technologies—Beijing's influence over the internet's physical backbone is growing.

The economic impact of internet disruptions on highly connected economies is substantial. For instance, the NetBlocks Cost of Shutdown Tool (COST) estimates the economic impact of internet disruptions using indicators from the World Bank, ITU, Eurostat, and the U.S. Census. According to data presented by Atlas VPN, based on NetBlocks' COST tool, a global internet shutdown for one day could result in losses of about $43 billion, with the United States and China accounting for nearly half of this sum. Additionally, Deloitte has estimated that for a highly internet-connected country, the per-day impact of a temporary internet shutdown would be on average $23.6 million per 10 million population.

A deliberate attack on routing protocols could cause widespread financial and operational chaos. In today's interconnected world, where digital infrastructure underpins economic stability, the ability to manipulate undersea cable traffic represents a subtle but powerful geopolitical weapon.

Addressing this threat goes beyond simply building more cables. It requires rethinking how routing protocols are governed. Transparent global standards must ensure no single country or company can dominate these systems. Routine independent audits should be conducted to detect anomalies that may signal interference. Efforts like the European Union's Global Gateway initiative and Japan's Digital Partnership Fund must focus on creating alternative routes to reduce reliance on Chinese-controlled nodes.

This issue highlights a new reality in global politics: control over data flows is becoming a key form of power. While most attention has been on building physical infrastructure, the quiet manipulation of routing protocols marks an equally profound shift in global influence. To protect the integrity of the internet, the world must act decisively at both technical and governance levels.

Fiber-Optic Cable Repair Networks

China's disproportionate control over fiber-optic cable repair networks reveals potential vectors for intelligence dominance, coercive leverage, and disruption of digital sovereignty. Globally, an estimated 60 dedicated cable repair ships service the planet's 1.5 million kilometers of submarine cables. China controls a substantial percentage of the fleet, including ships operated by state-affiliated enterprises like Shanghai Salvage Company and China Communications Construction Group. In contrast, the United States and its allies maintain a small patchwork fleet, mostly concentrated in the North Atlantic and lacking coverage in the Indo-Pacific, where over 50 percent of global internet traffic routes through key subsea cables.

China's fleet is heavily concentrated in the South and East China Seas, regions critical to global connectivity due to chokepoints like the Singapore Strait and the Luzon Strait. With maritime exclusivity bolstered by China's claims in disputed waters, its repair ships have nearly unrestricted access to monitor, repair, or potentially tamper with cables under the guise of routine maintenance.

Repair missions involve exposing critical cable infrastructure, including repeaters, amplifiers, and branch units—hardware that boosts signal strength over long distances but also represents points of vulnerability. Chinese vessels are equipped with advanced robotic submersibles and precision cutting-and-splicing technologies, designed for repairs but capable of installing signal interception devices. Such tools could include optical fiber taps capable of harvesting unencrypted metadata or capturing latency patterns to infer sensitive traffic flow.

China's advancements in photonics and quantum communication technologies underscore its capacity to exploit these vulnerabilities. The Chinese Academy of Sciences has reported significant breakthroughs in quantum key distribution (QKD) systems, raising the possibility of developing quantum-based methods to crack encrypted data intercepted during repairs. Integration of AI-driven data sorting tools could automate the extraction and classification of intercepted information, rendering bulk data acquisition during repairs a strategic advantage.

The high seas, where many repair operations occur, are governed by fragmented international frameworks like the United Nations Convention on the Law of the Sea (UNCLOS), which inadequately regulate activities involving critical infrastructure. The International Cable Protection Committee (ICPC) provides voluntary guidelines for repair operations, but enforcement mechanisms are weak, leaving the system vulnerable to exploitation by state actors.

Repair missions are often classified as “emergency operations,” requiring expedited approvals that bypass detailed oversight. In one case, a cable break in the South China Sea in 2021 prompted Chinese repair ships to operate without transparency for over three weeks, raising concerns about potential covert activities. These incidents are rarely reported, as they fall outside the jurisdiction of most maritime monitoring bodies.

The lack of countermeasures by the United States and its allies amplifies the risks posed by China’s dominance. The U.S. Navy operates no specialized repair ships, relying on private operators like Global Marine Group, whose fleet is aging and ill-equipped for operations in contested waters. This contrasts with China’s state-backed model, integrating its repair fleet into broader maritime networks, providing dual-use functionality for civilian and military objectives.

The financial model of undersea cable operations further constrains Western responses. Submarine cables are predominantly privately owned, with firms like Google, Meta, and Amazon investing heavily in infrastructure but lacking incentives to prioritize geopolitical considerations. This privatization leaves strategic gaps in surveillance and monitoring, as governments must negotiate access to privately controlled repair missions.

To mitigate China’s strategic advantage, a multipronged response is essential. The United States and its allies must develop state-owned or state-subsidized repair fleets to operate in contested regions like the South China Sea and Indian Ocean. Enhanced maritime surveillance systems, such as underwater drones and sonar-based monitoring arrays, should be deployed to track repair ship movements in real time.

Revising international frameworks by expanding ICPC mandates to include mandatory reporting of repair operations could curb opacity. Collaboration with regional partners, particularly nations in the Quad (Australia, India, Japan, and the United States), could bolster collective maritime domain awareness and create redundancies in cable repair capabilities.

Maritime Data Through Automated Vessel Tracking

China’s exploitation of automated vessel tracking systems exemplifies a sophisticated component of its global digital strategy. At the heart of this initiative lies the Automatic Identification System (AIS), a maritime safety technology mandated by the International Maritime Organization (IMO) for vessels exceeding 300 gross tons engaged in international trade. While originally intended to improve navigational safety by broadcasting vessel identities, locations, courses, and cargo details, AIS has been effectively repurposed by Beijing into a dual-use asset that supports both economic intelligence gathering and military surveillance.

Chinese firms, including the BeiDou Navigation Satellite System and Alibaba Cloud, have developed advanced platforms that aggregate AIS transmissions from shipping lanes worldwide. These platforms integrate AIS data with artificial intelligence-driven predictive analytics, enabling Beijing to monitor and analyze global maritime chokepoints such as the Strait of Malacca, the Panama Canal, and the Suez Canal—key arteries of international commerce. By doing so, China gains critical insights into global shipping patterns, strategic trade routes, and supply chain dynamics. As of 2023, the global merchant fleet comprised around 60,000 ships.

During the 2021 Suez Canal blockage, Chinese logistics firms, leveraging real-time AIS data, rapidly identified alternative routes through the Arctic and along the Indian Ocean, allowing Chinese exporters to reroute goods while Western competitors faced delays. Similarly, in the Strait of Malacca, a waterway facilitating the transit of over 16 million barrels of oil daily and 40 percent of global trade, Chinese analysts have used AIS data to optimize resource flow, preempt congestion, and study vulnerabilities in energy supply routes.

AIS data plays a pivotal role in China's military strategy, especially in the Indo-Pacific. By combining AIS information with satellite imagery and data from undersea acoustic arrays, China has established a surveillance network capable of tracking naval deployments with precision. AIS data has been used to monitor patrol patterns of the U.S. Navy's Seventh Fleet, revealing that over a third of its South China Sea operations in 2022 followed predictable routes. This surveillance allows the People's Liberation Army Navy (PLAN) to anticipate U.S. Freedom of Navigation Operations (FONOPs) and position its assets accordingly.

China's manipulation of AIS extends to conflict simulations and asymmetric warfare. During military exercises near Taiwan in 2023, Chinese forces reportedly deployed unmanned surface vessels programmed to mimic civilian AIS signals, complicating the identification of hostile assets.

Through its Digital Silk Road initiative, Beijing has exported various forms of maritime technologies that incorporate Automatic Identification System (AIS) capabilities. China often provides financial incentives to promote the adoption of its technologies abroad, which may enhance its access to regional maritime data. This asymmetry grants China an informational advantage and risks reshaping maritime transparency norms in its favor.

Rare Subsea Mapping Data

China's increasing investment in subsea mapping has positioned it as a significant player in oceanographic intelligence, impacting scientific, commercial, and military domains. China has been actively mapping its claimed maritime territories using state-funded research vessels and autonomous systems. These efforts contribute to international initiatives like the Nippon Foundation-GEBCO Seabed 2030 project, which aims to map the entire global seabed by 2030 and had mapped approximately 23.4 percent as of June 2022 with international contributions. China's activities extend to strategic regions in the Indo-Pacific, the Arctic, and the Indian Ocean, raising concerns over the dual-use potential of its data collection.

Subsea mapping data is critical for submarine cable routing, undersea infrastructure development, and naval operations. China's repository of high-resolution bathymetric maps—including surveys of key chokepoints like the Strait of Malacca and the Bashi Channel—provides a tactical edge. These chokepoints are vital for global trade and serve as strategic naval passages for power projection and anti-access/area-denial operations. The People's Liberation Army Navy uses seabed data to optimize the placement of undersea sensor arrays, critical for its "Great Underwater Wall" initiative, integrating hydroacoustic monitoring to detect foreign submarines.

China's advancements in autonomous underwater vehicles (AUVs) enhance its capabilities. In 2021, the Hailong III and Qianlong II AUVs were deployed for deep-sea mapping missions in the South China Sea, gathering data at depths over 6,000 meters. These AUVs have multi-beam sonar systems achieving sub-meter resolution, surpassing commercial standards. Their ability to operate autonomously over long durations allows China to map intricate undersea topographies critical for resource exploration and undersea warfare.

China has used seabed mapping as a diplomatic tool to extend influence over smaller nations. Through its Maritime Silk Road Initiative, Beijing has signed agreements with over 20 countries, granting Chinese research vessels access to Exclusive Economic Zones

(EEZs). Between 2015 and 2022, Chinese expeditions in Pacific Island nations' EEZs often involved dual-use mapping activities.

In 2019, the Chinese survey vessel Haiyang Dizhi 8 conducted seismic surveys near the Vanguard Bank within Vietnam's Exclusive Economic Zone (EEZ), collecting bathymetric data that aligns with key undersea routes potentially useful for submarine operations. This incursion led to a tense standoff with Vietnam, drawing international criticism over China's assertive actions and raising concerns about the dual-use potential of the data collected. Similarly, in 2018, China's proposed involvement in undersea cable projects connecting Papua New Guinea and the Solomon Islands through Huawei Marine raised significant security concerns. Fearing risks to the security of undersea communication cables and potential espionage, Australia intervened by funding and undertaking the projects themselves, highlighting apprehensions about granting Chinese entities access to critical seafloor data in the region.

China's seabed mapping strategy has significant military implications, particularly in the South China Sea. In this region, where China has constructed artificial islands such as Fiery Cross Reef, Subi Reef, and Mischief Reef, high-resolution seabed data enables precise deployment of missile systems, naval patrols, and underwater drones. Detailed seabed mapping supports the construction and fortification of these islands, allowing for the installation of surface-to-air missiles, anti-ship cruise missiles, and the operation of military airstrips. Additionally, China's deployment of unmanned underwater vehicles like the Sea Wing (Haiyi) gliders enhances their ability to collect oceanographic data crucial for submarine navigation and anti-submarine warfare. These activities have raised concerns among neighboring countries and the international community about the dual-use potential of China's maritime endeavors and their impact on regional security.

By controlling seabed mapping data, China influences submarine cable networks, which carry 95 percent of global internet traffic and $10 trillion in daily financial transactions. China's involvement in projects like the South Pacific Cable Project through state-owned

China Mobile led to concerns over data interception capabilities. Its presence in Arctic seabed mapping, facilitated by icebreaker vessels like Xuelong 2, underscores ambitions to secure alternative maritime routes and resources under the guise of scientific research.

China's approach to subsea mapping data has raised concerns about transparency and shared access in the global community. While international initiatives like the Seabed 2030 Project encourage open sharing of ocean floor data to advance scientific research and environmental understanding, China has been criticized for not fully sharing the extensive seabed data it collects. For example, much of the data gathered by Chinese vessels in international waters is not readily available in global databases like those managed by the International Hydrographic Organization (IHO) or the General Bathymetric Chart of the Oceans (GEBCO). This selective sharing limits other nations' ability to leverage valuable information and contrasts with global norms promoting cooperation and transparency in oceanographic research.

From RealClearWire

Views expressed in this article are opinions of the author and do not necessarily reflect the views of The Epoch Times.

OPINION

Carlo J.V. Caro

Author

Carlo J.V. Caro has a master's degree from Columbia University and is a political and military analyst.