YOUNG LEADERS
PROGRAM

UNDERWATER FRONTLINES: CHINA'S CABLE-CUTTING THREAT IN THE SOUTH CHINA SEA

BY ROCCO CARTUSCIELLO

Rocco Cartusciello *is the current Chapter Head for Washington, D.C. He holds a Masters in Asian Studies from Georgetown University and researches indo-pacific technology supply chains.* .

Photo: Undersea cables. Source: CircleID

In March 2025, China unveiled a deep-sea cable-cutting ship capable of slicing through the world's most reinforced undersea infrastructure. Developed by the China Ship Scientific Research Centre (CSSRC), the ship marks a strategic shift.

Undersea cables—carrying over 99 percent of global digital traffic—are now prime targets in gray zone warfare. These networks support military coordination, financial markets, and digital infrastructure. As tensions rise in the South China Sea, subsea cables face growing vulnerability to Chinese coercion.

The region contains a dense network of undersea fiber-optic cables that channel Asia-Pacific internet traffic. China's gray zone tactics have increasingly targeted these cables. In early 2025, disruptions between Taiwan and its offshore islands were linked to Chinese vessels like the Xingshun 39 and Hongtai 58, operating under deceptive identities. Similar incidents have occurred in the Taiwan Strait and Baltic Sea.

The subsea cable industry is dominated by four major private firms: SubCom (U.S.), Alcatel Submarine Networks (France), Nippon Electric Company (Japan), and HMN Technologies (China, formerly Huawei Marine). These companies, often in partnership with telecom providers and tech giants like Amazon and Google, are responsible for the vast majority of undersea cable manufacturing and installation.

Subsea cables work by transmitting data as pulses of light through single-mode optical fibers. These fibers are housed inside protective tubes, surrounded by shock-absorbing gel, wrapped in steel wires for tensile strength, and coated with copper tape to conduct electricity that powers undersea repeaters. An outer polyethylene layer insulates the structure from seawater. In higher-risk or shallower waters, cables are reinforced with additional armor, including extra steel sheathing and bitumen coatings, to resist corrosion, pressure, and physical damage from anchors or fishing gear.

Despite these reinforcements, cables are physically vulnerable on the seabed to natural disasters, ship anchors, and deliberate sabotage. While most cuts have historically been accidental, such as those caused by anchoring or fishing gear, recent incidents—particularly around Taiwan—suggest a shift toward intentional interference. This growing pattern indicates that sabotage, rather than accident, may increasingly account for cable disruptions.

Taiwan, the Philippines, and the U.S. are linked by both bilateral and trilateral cable systems, which all path in some way through the contested waters. Taiwan and the Philippines are connected via APCN-2, Apricot (planned for 2027), EAC-C2C, and Southeast Asia-Japan Cable. The Philippines and U.S. share Asia-America Gateway, Bifrost (2025), JUPITER, SEA-US, and Tata TGN Pacific. Taiwan and the U.S. are connected via E2A, FASTER, ORCA, and the Trans-Pacific Express Cable System. Notably, the Pacific Light Cable Network and TPU systems link all three—highlighting their shared strategic stake in subsea infrastructure and heightened vulnerability.

The inclusion of the Philippines' here stems from its geographic location and digital ties with the U.S. and Taiwan. Its participation in systems like PLCN and TPU creates both resilience and exposure. As it integrates further into regional defense structures, Manila's relevance in protecting digital infrastructure in contested waters continues to grow.

Guam has also become a key chokepoint, primarily for the U.S. It hosts 15 operational cables with four more currently underway, underscoring its value as a secure Pacific hub. Strategically, Guam functions as one of America's principal digital and communications gateways into Asia, serving both civilian and military networks. Its central location makes it a natural transit point for trans-Pacific data and a focal point in U.S. infrastructure planning for the Indo-Pacific.

In response to Chinese obstruction, countries like Vietnam have rerouted planned infrastructure to avoid contested areas—raising costs but reducing risk. With the advent of new cable-cutting technology and rising tensions, current projects, like Apricot, E2A, or ORCA, may experience delays or even result in redirections.

China's new vessel reportedly operates at depths of 4,000 meters and features a tool capable of cutting armored cables. It uses a six-inch diamond-coated grinding wheel spinning at 1,600 rpm—powerful enough to breach reinforced sheaths with minimal seabed disturbance. Originally designed for deep-sea mining, it can exceed the depth of most cable infrastructure, giving Beijing plausible deniability while potentially enabling strategic disruption.

As part of an effort to mitigate these gray zone tactics, organizations like the International Cable Protection Committee (ICPC) foster consistent stakeholder coordination. Taiwan has also taken further steps: passing new telecom laws, designating key cables as critical infrastructure, deploying automatic ship warning systems (SAWS), and boosting Coast Guard oversight. However, the industry's commercial nature limits proactive state involvement—especially in low-return zones.

Addressing these risks requires coordinated international action. Nations must recognize that the protection of digital infrastructure is no longer a niche concern—it is central to national security, economic stability, and strategic autonomy. Countries must build more cables, improve redundancy, and treat cable protection as a core security priority rather than a secondary commercial concern. The U.S. and its allies are already rerouting projects to avoid disputed waters, reflecting the growing recognition of these vulnerabilities. As China advances its capabilities and refines its gray zone strategies, a strong, integrated, and persistent public-private response is vital to defend the digital lifelines that increasingly underpin the functioning of the global order and the free flow of information in the twenty-first century.