G1VE TECHNOLOGIES

The Seabed is a Frontline Now: Why Undersea Cables Are Becoming the Most Underprotected Layer of National Security

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP

Jul 13, 2026

Original source

https://www.linkedin.com/pulse/seabed-frontline-now-why-undersea-cables-becoming-w-b--2w6ve/

I. The Most Consequential Critical Infrastructure In The World Is Also The Least Visible

Ask most executives, board members, or even elected officials to describe critical infrastructure, and they will list power grids, water treatment, telecommunications, ports, financial rails, hospitals, and pipelines. Rarely, if ever, will they mention the undersea fiber-optic cable network on the seabed. That omission is dangerous. Subsea cables carry more than 95 percent of international data, connecting continents, powering global commerce, and enabling everything from diplomatic traffic and military orders to $10 trillion in daily financial transactions. This is not backbone infrastructure. It is the backbone of the backbone.

A separate Center for Strategic and International Studies (CSIS) analysis puts the picture in even sharper terms: roughly 600 cables are planned or operational worldwide, spanning approximately 1.2 million kilometers; one major international bank alone moves an average of $3.9 trillion daily through these systems; and roughly 98 percent of the world's undersea cables are manufactured and installed by only four private firms. Amazon , Google , Meta , and Microsoft together own or lease around half of all undersea bandwidth worldwide. That is not just infrastructure concentration. That is strategic gravity.

If a peer adversary wanted to hit U.S. and allied economic, military, and intelligence throughput without firing a shot into sovereign land, the seabed is exactly where they would go. In 2026, they already are.

II. The UK Just Made The Covert Threat Explicit

In April 2026, UK Defense Secretary John Healey did something rare in undersea-cable security: he said the quiet part out loud. The UK publicly accused Russia of a covert, month-long operation involving an Akula-class attack submarine and a pair of GUGI surveillance submarines, all tracked in and around British waters. Healey said the sister GUGI vessels spent time over "critical infrastructure relevant to us and our allies in the North Atlantic." He warned there would be "serious consequences" for any attempt by Moscow to damage subsea infrastructure.

The operational tempo required to track that activity was significant. A single Royal Air Force P-8 Poseidon logged over 450 flight hours. A Type 23 frigate covered several thousand nautical miles. Sonobuoys were deployed. Norway contributed a P-8 and a frigate. In simple mission-assurance terms: it took a coalition-scale ISR and maritime patrol commitment just to monitor one Russian deployment. That is a scarce-resource picture. The Royal Navy has been called "hollowed out" after years of underinvestment. NATO allies had to stitch coverage together in real time.

The critical framing from FDD analyst John Hardie, cited in that reporting, is that GUGI vessels are specifically designed to survey underwater infrastructure during peacetime and sabotage it in conflict. That single sentence should reshape how national-security leaders think about the seabed. It is not neutral space. It is contested space. It is a peacetime-mapping, wartime-cutting environment.

III. This Is Not Just A Russia Problem

The exposure is global. Center for Strategic and International Studies (CSIS) notes chokepoints in the Red Sea and the South China Sea — precisely where Houthi attacks and Chinese maritime activity have created ambient risk to critical cable arteries. In 2023, Taiwanese authorities publicly accused two Chinese vessels of cutting the two cables supplying internet to the Matsu Islands. Cables are severed by accident 100 to 150 times per year globally, mostly from anchors and fishing gear, which means adversaries can hide deliberate action inside a fog of common accidents. That is a classic gray-zone playbook.

There is also the repair-fleet vulnerability. Repair ships are aging. Overreliance on Chinese repair capacity — particularly through HMN Tech , which prices bids 20 to 30 percent below Western rivals and has become the world's fastest-growing subsea cable builder over the past decade — creates a strategic dependency in the exact moment when maintenance access might matter most. A new cable ship costs over $100 million to build, repairs run $1 to $3 million per incident, and new projects cost $30,000 to $50,000 per kilometer. The economics do not lie. Repair capacity is the second frontline.

For U.S. leaders, this is not an obscure telecom issue. It is a national-security, national-intelligence, and mission-continuity issue that touches JADC2 data flows, IC communications, financial-system resilience, joint force sustainment, and coalition operations across every combatant command with a maritime seam.

IV. What Subsea Disruption Actually Does To National Power

The historical example from Center for Strategic and International Studies (CSIS) is a punch to the sternum: after undersea cable breaks between Egypt and Italy in 2008, U.S. drone flights in Iraq dropped from hundreds a day to tens a day. That is what one degraded artery can do to a live operational picture. In 2026, with the U.S. dependent on subsea cables for diplomatic cables, military orders, IC traffic, financial rails, cloud services, undersea SIGINT support, and increasingly 5G-enabled command and control, the fragility multiplies. As military applications of 5G and autonomous systems grow, so does subsea dependence.

A serious adversary does not need to sever the entire network. It only needs to degrade the right cables, at the right chokepoints, at the right moment. That is why the seabed matters to mission command, to sustainment, to logistics, to ISR, to JP 4.0-style logistical resilience, to critical infrastructure protection, and to any joint or combined operation that depends on continuous data flow across theaters.

Undersea cables are also physically and digitally vulnerable — cut, tapped, network-manipulated, or "kill-clicked" by manipulating cable management systems. The threat surface spans submarines, spy ships, autonomous vessels, insiders at landing stations, and cyber intrusions into terrestrial management infrastructure. This is not a single-vector defense problem. It is a multi-domain, all-service, all-agency problem.

V. Where U.S. Policy Is Still Lagging

For all the CI Fortify progress at Cybersecurity and Infrastructure Security Agency and the new consequence-based cyber directives, sector coverage for the communications and financial services critical infrastructure sectors still under-treats subsea cables. Sen. Mark Warner's Combat Emerging Threats to Critical Infrastructure Act, which would force Cybersecurity and Infrastructure Security Agency to update sector cybersecurity plans across all 16 critical infrastructure sectors — some of which have not been meaningfully refreshed in over a decade — is a strong step, and it should absolutely include subsea explicitly.

Center for Strategic and International Studies (CSIS) 's recommendations are the right architecture. Increase intelligence sharing among allies on cable threats and cable projects. Promote rigorous national risk assessments — Team Telecom-style — for every new cable project touching the U.S. Ensure private-sector commitment through voluntary standards from the ICPC | International Cable Protection Committee (ICPC), backed by mandatory floors where necessary. Fund U.S. and allied repair capacity aggressively, including a healthier Cable Security Fleet and additional repair ships. Streamline U.S. permitting, which can currently take up to two years. Coordinate diplomatically through Quad-Plus, Data Free Flow with Trust, and other frameworks to counter state-subsidized Chinese cable expansion. Complete a stronger international legal framework so cables are not treated as fair-game targets in wartime under UNCLOS gaps.

VI. What The Joint Force Should Own And What Industry Must Fund

For the US Navy , U.S. Coast Guard , United States Space Force , U.S. Pacific Command , U.S. European Command , U.S. Northern Command , USSOCOM , and the intelligence community, subsea protection is a mission set that spans all six warfighting domains touching the sea, the seabed, cyberspace, and the electromagnetic spectrum. AUKUS partners already signed an agreement in May 2026 on underwater drones and accelerated submarine plans that will develop payloads, sensors, and weapons deployable across the three nations' UUV fleets — specifically citing detection, deterrence, and response for maritime threats including those against underwater cables and pipelines. That is directional. It is not sufficient.

Private industry — the hyperscalers, the telecom operators, the cable consortia, and the financial sector — must move from passive infrastructure ownership to active resilience. That means redundant routing, satellite backup for critical flows, hardened landing stations, tabletop exercises with government partners, insider-risk programs at repair-vessel operators, cryptographic protections for network management, and standardized incident-response coordination with Cybersecurity and Infrastructure Security Agency , sector risk management agencies, the US Navy , and the U.S. Coast Guard .

Governors, state adjutants general, National Guard Bureau cyber commands, and homeland-security operators also need to understand where landing stations sit in their jurisdictions and what happens to their state economies if those stations degrade during a crisis. This is not a coastal-state issue. It is a national issue with coastal-state consequences.

VII. What Leaders Should Do Next

If you lead in this space, five moves matter now.

First, know your subsea dependence. Map which of your organization's operations rely on transoceanic data flow — cloud, SaaS, IC traffic, financial rails, logistics ERP, or coalition command. If you cannot list them, you cannot defend them.

Second, rehearse degraded operations. Assume cable-level disruption. Assume repair delay. Assume satellite backup is partial. Test what breaks first.

Third, fund repair and monitoring capacity. This is one of the rare national-security investments where the return curve is obvious. Cable ships, autonomous underwater sensors, sonar arrays, and hardened landing stations are cheap compared to the disruption they prevent.

Fourth, treat cable network management as a cyber crown jewel. Landing stations, cable management systems, and NOC access are strategic terrain. Protect them accordingly.

Fifth, fold subsea explicitly into every critical infrastructure sector plan update. If Warner's bill passes, this becomes possible. Even if it does not, agencies and operators should refuse to pretend cables are "someone else's problem." They are everyone's problem.

VIII. Thought-Provoking Close: The Final assessment

The seabed is a frontline now. That is not rhetoric. It is a description of how peer adversaries are already operating, how much of the global economy already depends on the cables they are mapping, and how little redundancy exists if the wrong lines go dark at the wrong moment.

Serious leaders will stop treating undersea cables as invisible plumbing and start treating them as strategic infrastructure worthy of joint-force attention, coalition doctrine, industrial resilience, and executive urgency. The rest will find out the hard way — probably at 3:17 a.m., during a crisis, with the wrong latency on the wrong dashboards.

✨ Call to Action: Step Into the Arena ✨

Most professionals will read about the future. A select few will shape it.

If you are serious about staying ahead of the curve in Artificial Intelligence, Regulatory Compliance, and Enterprise Risk, this is where you need to be.

📩 Subscribe to Securing Our Future to gain direct access to:

1. Strategic foresight on AI Governance & Ethical Deployment
2. Real-world applications across National Security & Mission Assurance
3. Advanced GRC, TPRM, and Regulatory Compliance frameworks
4. Emerging Fintech and Risk Intelligence innovations

⚔️ The landscape is shifting—fast. The gap between those who understand and those who execute is widening.

This is built for professionals responsible for decisions that carry consequence—not commentary.

📅 Ready to operationalize these insights and move beyond theory?

👉 https://calendly.com/g1ve-technologies

Let us translate insight into measurable, defensible outcomes—and build capability, not just conversation.

🔍 About the Author

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP is a National Security-aligned Artificial Intelligence Strategist/Tactician and Governance, Risk, and Compliance (GRC) Authority/Subject Matter Expert with over a decade of experience operating at the intersection of National Security, National Defense, Critical Infrastructure, Cybersecurity, AI Governance, Mission Assurance, Mission-Critical Systems, and Predictive Funding/Grant Intelligence.

As Managing Partner at G1VE Technologies, LLC and a Strategic Board Advisor, W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP architects and operationalizes enterprise-scale risk, compliance, and AI governance ecosystems across both Public and Private Sector environments—including Fortune 500/1000 organizations and Federal-aligned missions, where failure is not an option.

His work is centered on delivering Decision Advantage, strengthening Operational Resilience, and enabling organizations to navigate high-stakes, high-uncertainty environments with precision and confidence.

📡 Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP here to stay at the forefront of:

- Artificial Intelligence
- National Security
- GRC
- Cyber Risk
- Regulatory Strategy
- Mission Assurance