Deterring Cable Sabotage in the AI Era

KEVIN FRAZIER*

The resilience of the undersea cable system determines the ceiling of the United States' artificial intelligence (AI) ambitions. As AI laboratories and hyperscalers invest hundreds of billions in computing and data centers, the physical infrastructure linking those resources to global networks has become a strategic vulnerability. Undersea cables—responsible for carrying nearly all transoceanic data—remain inadequately protected, governed by outdated statutes, and increasingly targeted by state and nonstate actors wielding emerging technologies such as autonomous undersea vehicles. This Essay argues that safeguarding the nation's AI competitiveness requires treating cable security as a foundational priority of national power rather than a niche maritime concern.

Drawing on evidence of accelerating threats, from Iranian uncrewed undersea vehicles to routine breakages caused by fishing, anchors, and coastal chokepoints, the Essay develops a deterrence-centered framework capable of addressing both intentional sabotage and the far more common operational faults that already strain the system. It calls for a two-pronged strategy. First, the United States must execute an ambitious long-term "sea shot" to expand repair capacity, deploy autonomous monitoring systems, and build or retrofit large segments of the global network. Second, Congress should enact immediate legal and regulatory reforms that

* Kevin Frazier directs the AI Innovation and Law Program at the University of Texas School of Law and is a Senior Fellow at the Abundance Institute. Sven Lohse provided excellent research assistance on this Article.

raise the cost of attacks, expand detection capabilities, and decrease the probability that any attempted disruption succeeds. These measures include overhauling the Submarine Cable Act, conditioning landing licenses on the adoption of advanced sensing and reporting technologies, establishing cable protection zones, strengthening construction and burial standards, mandating redundancy through diverse routing, and ensuring long-term access to repair ships.

Collectively, these reforms would shift the strategic calculus of adversaries while reinforcing the operational backbone of the AI economy. As data-intensive applications—from military logistics to financial markets to disaster response—become increasingly sensitive to latency and downtime, even short outages could impose cascading harms across society. A cable system designed for a pre-AI era cannot sustain twenty-first-century demands. By modernizing legal authorities, accelerating technological upgrades, and elevating deterrence as a guiding principle, Congress can secure the connective tissue of the AI age and ensure that America's technological advantages rest on an infrastructure as resilient as the ambitions it seeks to support.

INTRODUCTION

A robust undersea cable system is an essential part of achieving the nation's AI aspirations and, therefore, a target of adversaries also in pursuit of AI dominance. Inadequate attention to this critical infrastructure risks jeopardizing the substantial investments being

made in AI and related technologies.[1] Consider, for example, that U.S. hyperscalers spent around $371 billion on data centers and computing resources in 2025 alone and anticipate spending more in the future.[2] As one representative of a major lab made clear, "without the connectivity [via undersea cables] that connects those data centers, what you have are really expensive warehouses."[3] A failure to adequately maintain and protect the undersea cable system may also expose the United States and its allies to significant economic, political, and technological disruptions.[4] It follows that the scale and scope of AI ambitions rise and fall with our attention and commitment to the numerous and growing threats to our undersea cable system.[5]

There is no backup plan. If all or even a significant number of the twenty or so cables connecting Europe to North America were

---

[1] *See* Tim Stronge, *Do $10 Trillion of Financial Transactions Flow over Submarine Cables Each Day?*, TELEGEOGRAPHY (Apr. 6, 2023), https://blog.telegeography.com/2023-mythbusting-part-1 [https://perma.cc/DGM5-B4YL].

[2] Martin Stansbury et al., *Can US Infrastructure Keep up with the AI Economy?*, DELOITTE RSCH. CTR. FOR ENERGY & INDUS. (June 24, 2025), https://www.deloitte.com/us/en/insights/industry/power-and-utilities/data-center-infrastructure-artificial-intelligence.html [https://perma.cc/H2FA-4NKV]; Eli Tan, *Meta Raises Its Spending Forecast on A.I. to Above $70 Billion*, N.Y. TIMES (Oct. 29, 2025), https://www.nytimes.com/2025/10/29/technology/meta-spending-ai.html [https://perma.cc/F6C6-3G2C].

[3] Magdalena Petrova, *Underwater Cables Are a Vital Piece of the AI Buildout and Internet—Investment Is Booming*, CNBC (Nov. 8, 2025, at 08:00 ET), https://www.cnbc.com/2025/11/08/big-tech-ai-underwater-cables.html [https://perma.cc/Y4PC-L635] (quoting Alex Aime, Vice President of Network Investments at Meta).

[4] *See* JOCELINN KANG & JESSIE JACOB, AUSTL. STRATEGIC POL'Y INST., CONNECTING THE INDO-PACIFIC: THE FUTURE OF SUBSEA CABLES AND OPPORTUNITIES FOR AUSTRALIA 5 (Sep. 2024), https://aspi.s3.ap-southeast-2.amazonaws.com/wp-content/uploads/2024/10/28023544/Connecting-the-Indo-Pacific.pdf [https://perma.cc/45HC-H4BW] (detailing how even a few undersea cable faults can wreak havoc on connected nations, especially those with comparatively few cables).

[5] *See* Kevin Frazier, *Wired for Failure: The Undersea Cable Emergency That Could Sink America's AI Aspirations*, LAWFARE (Sep. 16, 2025, at 09:55 ET), https://www.lawfaremedia.org/article/wired-for-failure--the-undersea-cable-emergency-that-could-sink-america-s-ai-aspirations [https://perma.cc/5FM5-DGMC].

disrupted,[6] for example, satellites would not serve as a viable alternative. Internet traffic travels drastically slower via satellites.[7] The satellite network also has significantly less bandwidth.[8]

This reality merits a two-pronged response. The first is a "sea shot" that includes building ten new cable repair ships explicitly for use by the United States and its allies, deploying 100 autonomous undersea drones to gather critical information to maintain the undersea cable system, and laying or retrofitting 100,000 miles of undersea cables.[9] This prong is best thought of as an "offensive" strategy through which the United States can reassert its authority in this critical domain. It will require significant political buy-in, financial support, and time. Cable operators often take years to lay a new cable.[10]

---

[6] Alan Mauldin, *Cutting off Europe? A Look at How the Continent Connects to the World*, TELEGEOGRAPHY (Oct. 13, 2022), https://blog.telegeography.com/cutting-off-europe-a-look-at-how-the-continent-connects-to-the-world [https://perma.cc/JAZ9-WUWU]; *see* MIKE CONSTABLE, LANE BURDETTE & ALAN MAULDIN, THE FUTURE OF SUBMARINE CABLE MAINTENANCE: TRENDS, CHALLENGES, AND STRATEGIES 34 (June 2025), https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/The%20Future%20of%20Submarine%20Cable%20Maintenance_%20Trends%2C%20Challenges%2C%20and%20Strategies.pdf [https://perma.cc/K9AM-9QEY] (forecasting as many as twenty-five trans-Atlantic cables by the year 2040).

[7] *Submarine Cable Frequently Asked Questions*, TELEGEOGRAPHY, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions [https://perma.cc/Z3EC-55DX] (last visited Nov. 15, 2025); INSIKT GRP., SUBMARINE CABLES FACE INCREASING THREATS AMID GEOPOLITICAL TENSIONS AND LIMITED REPAIR CAPACITY 18 (2025), https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-2025-0717.pdf [https://perma.cc/FT5A-Z78T] ("[A] trans-pacific fibre-optic call need only travel about 5,000 miles point-to-point, compared to a satellite call, which must travel 22,235 miles from the Earth to a satellite and then another 22,235 back.") (internal quotation marks omitted).

[8] Alan Mauldin, *Will New Satellites End the Dominance of Submarine Cables?*, TELEGEOGRAPHY (July 1, 2019), https://blog.telegeography.com/will-new-satellites-end-the-dominance-of-submarine-cables [https://perma.cc/2VZU-QMR2]; *The Battle for Bandwidth: Submarine Cable and Broadband Satellite Data*, NEW SPACE ECON., https://newspaceeconomy.ca/2023/08/13/the-battle-for-bandwidth-submarine-cable-and-broadband-satellite-data/ [https://perma.cc/2UXT-FDNM] (last visited Feb. 25, 2026).

[9] *See* Frazier, *supra* note 5.

[10] *See* Jürgen Hatheier, *AI's Role in Revolutionizing Submarine Network Connectivity*, RCR WIRELESS NEWS (Aug. 9, 2024), https://www.rcrwireless.com/20240809/network-infrastructure/ais-role-in-revolutionizing-submarine-network-connectivity-reader-forum [https://perma.cc/5YVV-YYRT] ("[T]hese

Construction of a new undersea cable repair ship can take as many as five years.[11] Those delays mean that the United States should pursue a second, "defensive" prong of this strategy in the interim. This prong involves the immediate adoption of policy strategies that deter bad actors from attacking the undersea cable system.

I. INCREASED DETERRENCE AS AN IMMEDIATE PRIORITY

Deterrence is a function of three variables: the costs of an attack, the likelihood of its success, and the magnitude of its success. Bad actors will have little reason to attempt to sabotage the undersea cable system if doing so is expensive, difficult, or inconsequential. Critically, the same tools used to deter intentional sabotage will also make the undersea cable system more resilient to the more frequent causes of cable faults, which also merit due consideration. As recommended by the International Cable Protection Committee (ICPC), undersea cable policy should be driven by evidence, not speculation or exaggeration.[12] Dragged anchors account for about thirty percent of all breaks.[13] More generally, most breaks occur due to fishing and other human activities.[14] Any short-term solution should be evaluated for its responsiveness to both emerging issues, such as sabotage, and these more common causes of breaks.

---

are projects that cost in the hundreds of millions of dollars and take years to plan and deploy.").

[11] CONSTABLE, BURDETTE & MAULDIN, *supra* note 6, at 67.

[12] *See* INT'L CABLE PROT. COMM., GOVERNMENT BEST PRACTICES FOR PROTECTING AND PROMOTING RESILIENCE OF SUBMARINE TELECOMMUNICATIONS CABLES 1 (2024), https://www.iscpc.org/documents/?id=3733 [https://perma.cc/D88X-HDSS] (recommending that submarine cable resilience policies prioritize statistically significant risks and data-informed risk assessment).

[13] *Damage to Submarine Cables from Dragged Anchors*, INT'L CABLE PROT. COMM.: ICPC VIEWPOINTS (Feb. 24, 2025), https://www.iscpc.org/publications/icpc-viewpoints/damage-to-submarine-cables-from-dragged-anchors/ [https://perma.cc/H9E5-KPNW].

[14] SUBMARINE TELECOMS F., INC., SUBMARINE TELECOMS INDUSTRY REPORT 2025–2026, at 167 (2025) [hereinafter INDUSTRY REPORT 2025–2026], https://subtelforum.com/submarine-telecoms-industry-report/ [https://perma.cc/EEL2-MU7W].

II. INCREASING THE COST OF SABOTAGE

The costs of attacking the undersea cable system involve the actual expenses of locating and breaking a cable in addition to the probability of being caught multiplied by the punishment. New technologies, such as autonomous undersea vehicles (AUVs), will decrease the costs of an attack.[15] For the sake of illustration, it appears as though Iran has already developed uncrewed undersea vehicles (UUVs) that are precisely designed to attack static targets.[16] What's more, Iran may have already made those tools available to the Houthi militant group.[17] Aerial drones have already transformed terrestrial conflicts by lowering the cost of destruction.[18] Iranian advances and their willingness to pass technology along to non-state actors suggest the same may be true in the undersea domain—to the extent it is not already.[19] The United States should respond by developing similar AUVs and UUVs—as called for under the "sea shot" described above, while also increasing its enforcement capabilities and punishments in the short run.

To start, Congress must amend the Submarine Cable Act of 1888 to, at a minimum, bring the fines for willfully or negligently breaking a cable into line with international norms and, ideally, to specify

---

[15] JOINT COMM. ON THE NAT'L SEC. STRATEGY, SUBSEA TELECOMMUNICATIONS CABLES: RESILIENCE AND CRISIS PREPAREDNESS, HC 723, HL Paper 179, 2024–26 Sess., at 10, 14 (UK 2025) [hereinafter UK REPORT], https://committees.parliament.uk/publications/49566/documents/264088/default/ [https://perma.cc/V3E6-XHFS] (citing Professor Rowlands' observation that advances in AUVs may increase the odds of attacks on multiple cables at once); Yuval Eylon, *The Challenge of Defending Underwater Communication Infrastructures*, INST. FOR NAT'L SEC. STUD. (June 29, 2023), https://www.inss.org.il/publication/under-water/ [https://perma.cc/Y96F-H42K] (warning of "[r]ecent state-of-the-art developments of underwater capabilities, such as long-range midget unmanned submersible vehicles and remotely controlled submarine robots").

[16] Ash Rossiter, *Cable Risk and Resilience in the Age of Uncrewed Undersea Vehicles (UUVs)*, 171 MARINE POL'Y 1, 1 (2025), https://www.sciencedirect.com/science/article/pii/S0308597X24004342 [https://perma.cc/4S93-UPAM].

[17] Rossiter, *supra* note 16, at 1, 3.

[18] *See* James Paterson, *High-Tech Drones Are Changing Warfare—Terrorists May Soon Follow the Same Playbook*, THE CONVERSATION (Aug. 12, 2025, at 01:13 ET), https://theconversation.com/high-tech-drones-are-changing-warfare-terrorists-may-soon-follow-the-same-playbook-262626 [https://perma.cc/49DQ-RLP8].

[19] *See* Rossiter, *supra* note 16, at 1, 3.

fines of an ever greater magnitude. The current fines are $5,000 and $500, respectively.[20] It is likely cheaper to intentionally break an undersea cable than to go on a holiday trip to Europe. In contrast, New Zealand imposes a $152,530 penalty on any person who breaks a cable regardless of intent.[21] Singapore has imposed a penalty on that scale, too;[22] in 2022, a private construction company faced a $220,000 fine for causing multiple telecommunication cables to break while working on a nearby project.[23] Australia may impose fines of nearly $27,000 for related offenses.[24] The United States should not dillydally in updating the Submarine Cable Act and sending a strong signal that it is ready and willing to hold bad actors accountable for their interference with this critical infrastructure. Many of the undersea cable breaks attributed to nations such as China and Russia have been carried out by commercial vessels in relatively shallow waters[25]—breaks that may fall within the ambit of the Submarine Cable Act if committed near the U.S. coast.

III. INCREASING THE ODDS OF DETECTION

To increase the odds of detecting responsible parties, Congress should condition any grant or renewal of a cable landing license

---

[20] *See* 47 U.S.C. §§ 21–22.

[21] Submarine Cables and Pipelines Protection Act 1996, s 11 (N.Z.) (stating that willfully or negligently damaging a submarine cable results in a fine of up to 250,000 NZD).

[22] *See* William Yuen Yee, *Laying Down the Law Under the Sea: Analyzing the US and Chinese Submarine Cable Governance Regimes*, JAMESTOWN (Aug. 4, 2023), https://jamestown.org/laying-down-the-law-under-the-sea-analyzing-the-us-and-chinese-submarine-cable-governance-regimes/ [https://perma.cc/2FUH-NEC2]. For a list of enforcement decisions by Singapore's Infocomm Media Development Authority, see generally *Damage to Telecommunication Cables*, INFOCOMM MEDIA DEV. AUTH.: ENF'T DECISIONS, https://www.imda.gov.sg/regulations-and-licensing-listing/competition-management/enforcement-decisions/damage-to-telecommunication-cables [https://perma.cc/UDQ4-XN3P] (last visited Mar. 3, 2026).

[23] Yee, *supra* note 22.

[24] *Id.*

[25] John Dotson, *Strangers on a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations*, JAMESTOWN (June 7, 2025), https://jamestown.org/strangers-on-a-seabed-sino-russian-collaboration-on-undersea-cable-sabotage-operations/ [https://perma.cc/C7ZK-ADPL].

upon the cable operator installing the latest sensing technologies and timely reporting any threats or anomalous activity. In the alternative, the cable operator can agree to a greater licensing fee to contribute to the ability of the U.S. government, including but not limited to the Coast Guard,[26] to track ships, submarines, and AUVs and UUVs. As an aside, fees collected by licensing authorities around the world should be explored as a means to gather funds necessary to solve some of the collective action problems that plague the undersea cable system.[27]

Every cable operator must secure a license from the Federal Communications Commission (FCC) prior to landing a cable in the United States.[28] Applicants must provide relatively little information to the FCC to satisfy statutory obligations.[29] Certain applications receive heightened scrutiny by the FCC and a number of other agencies with an interest in the nation's telecommunications network[30]—collectively known as "Team Telecom."[31] This group broadly examines whether granting a license would "pose a risk to national security or law enforcement interests of the United States."[32]

Even under this heightened review, it is unclear whether Team Telecom will obtain meaningful information about an operator's plans to adopt specific safeguards and to share specific information. For example, while applicants must answer "[w]hat provision will be made to monitor suspicious activity occurring over the paths of

---

[26] *Cf.* Madison L. Long, *Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks*, U.S. NAVAL INST.: PROCEEDINGS (May 2023), https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks [https://perma.cc/4KWC-N4N5] (contending that the U.S. Coast Guard should lead in efforts to protect the undersea cable system).

[27] Kevin Frazier, *Pooling Responsibility: Incentivizing Cable Owners to Safeguard the Global Undersea Network*, U. CIN. INTELL. PROP. & COMPUT. L.J. (forthcoming 2026).

[28] *See* 47 C.F.R. § 1.767 (2025).

[29] *See id.*

[30] Exec. Order No. 13,913, 85 Fed. Reg. 19,643, 19,645 (Apr. 8, 2020).

[31] Frazier, *supra* note 27.

[32] Exec. Order No. 13,913, 85 Fed. Reg. at 19,645.

the cables?,"[33] the response may not detail the information called for here. It is also not clear whether the applicant's answer to that question would be determinative in the decision to grant, renew, or deny a license. Though the FCC is in the process of amending and streamlining this process,[34] decisions by Team Telecom have been faulted as unpredictable for relying on a seemingly shifting set of standards and information.[35] Amid these reform efforts, the FCC—at the direction or encouragement of Congress—should factor this information into its review of all licenses.

Myriad new technologies can generate important information from undersea cables. Quantum sensing, for example, "could transform subsea cable monitoring by enabling accurate detection of environmental changes, underwater seismic activity, and potential threats like fishing trawls or sabotage."[36] Acoustic sensors may perform a similar function.[37] A German company has even developed a means to update existing cables with sonar-like technology that can determine if threats are nearby by "sens[ing] vibrations traveling through the water."[38] Which of these sensing technologies should be

---

[33] Second Report & Order at 14873, *In re* Process Reform for Exec. Branch Rev. of Certain FCC Applications & Petitions Involving Foreign Ownership, 36 FCC Rcd. 14848 (2021).

[34] Ari Q. Fitzgerald et al., *FCC Issues Submarine Cable Rules, Seeks Comment on Additional Proposals*, HOGAN LOVELLS (Sep. 16, 2025), https://www.hoganlovells.com/en/publications/fcc-issues-submarine-cable-rules-seeks-comment-on-additional-proposals [https://perma.cc/G8YV-E5QZ].

[35] Richard Salgado, *Undersea Cables, Hyperscalers, and National Security* 9 (Hoover Inst., Stan. Univ., Aegis Series Paper No. 2304, 2023), https://www.hoover.org/sites/default/files/research/docs/Salgado_finalfile_WebReadyPDF.pdf [https://perma.cc/H642-KVUH].

[36] Devon A. Johnson, *Into the Future: Quantum Technologies and the Impact on the Resilience of the Subsea Cable System*, SUBMARINE TELECOMS F. (Dec. 2, 2024), https://subtelforum.com/into-the-future-quantum-technologies-and-the-impact-on-the-resilience-of-the-subsea-cable-system/ [https://perma.cc/6JJZ-3P86].

[37] *See OptoDAS: The Leading Technology for Distributed Acoustic Sensing*, ALCATEL SUBMARINE NETWORKS, https://www.asn.com/fiber-sensing/ [https://perma.cc/LHV7-BQ9E] (last visited Nov. 15, 2025).

[38] Jowi Morales, *New Undersea Cable Tech Listens for Sabotage—Can Be Retrofitted to Existing Fiber Optic Lines*, TOM'S HARDWARE (Mar. 18, 2025), https://www.tomshardware.com/tech-industry/new-undersea-cable-tech-listens-for-sabotage-can-be-retrofitted-to-existing-fiber-optic-lines [https://perma.cc/AFR3-VWFA].

imposed on applicants warrants additional analysis by the FCC based on their costs and accuracy. The key is that "dumb" cables that provide little to no information to the operator and government become a thing of the past. Any information gathered by the sensors, such as any indications as to the current functionality of the cables,[39] then needs to be passed along to the relevant government authorities. Provision of more information about cables can inform ongoing policy decisions about how to increase the resiliency of the undersea cable system—decisions that are often made in the absence of full information.[40]

These two straightforward steps will alter the calculus of bad actors who often turn to commercial vessels to carry out attacks on their behalf. A more ambitious, though necessary, step involves designating cable protection zones, which would prohibit activities that interfere with the seabed from occurring in specified areas with a high density of cables.[41] Australia,[42] New Zealand,[43] and Denmark[44] are among the nations with such zones. The efficacy of this strategy turns on whether the state allocates sufficient enforcement resources to what may be a very difficult task of monitoring several zones. The United States could start by creating cable protection zones where there is already a high number of cables in a relatively finite geographic area. One place to start may be the north coast of Oregon. At least eight trans-Pacific cables go through that area.[45] This area

---

[39] *See* KANG & JACOB, *supra* note 4, at 21 (recommending that Australia likewise mandate the provision of such information).

[40] *See, e.g.*, UK REPORT, *supra* note 15, at 2 (highlighting the fact that additional information on how cable damage impacts cable operations would assist policy discussions).

[41] *See* Pierre Thévenin, *A Legislative Route to Combat Sabotage of Undersea Cables: A Q&A with Pierre Thévenin*, STOCKHOLM INT'L PEACE RSCH. INST. (Oct. 23, 2025), https://www.sipri.org/commentary/topical-backgrounder/2025/legislative-route-combat-sabotage-undersea-cables [https://perma.cc/U4VY-D89A] (including bottom trawling, dredging, and anchoring among such activities).

[42] *See* Telecommunications Legislation Amendment (Submarine Cable Protection) Bill 2013 (Cth) sch 3A (Austl.).

[43] *See* Submarine Cables and Pipelines Protection Act 1996, s 12 (N.Z.).

[44] *See* DANISH MAR. AUTH., ORDER NO. 939 OF 27 NOVEMBER 1992 ON THE PROTECTION OF SUBMARINE CABLES AND SUBMARINE PIPELINES § 1 (1992).

[45] *Submarine Cable Map*, TELEGEOGRAPHY, https://www.submarinecablemap.com/ [https://perma.cc/67WC-K7DF] (last visited Nov. 15, 2025) (reviewing map of submarine cables).

is also forecast to be especially prone to breaks in the coming years.[46] A combination of the Coast Guard, Air Force, Navy, and other authorities with resources to closely monitor ship traffic in that region could ensure a high enough degree of enforcement so as to deter bad actors from even attempting to sabotage those cables. Technological advances such as AI may make this monitoring all the easier[47] and justify creating such zones in other areas.[48]

IV. REDUCING THE ODDS OF SUCCESS

Congress can also drastically diminish the likelihood of a successful attack by imposing heightened responsibilities on cable operators to adopt best practices for laying more attack-resistant cables. The vast majority of cable breaks occur in shallow water, near shore, and in cable choke points.[49] Cable operators can implement several safeguards against such breaks. First, they can increase the armoring of cables.[50] Use of Kevlar to safeguard cables from sharks and other threats was once regarded as a novel tactic,[51] though its

---

[46] CONSTABLE, BURDETTE & MAULDIN, *supra* note 6, at 51.

[47] Matthew Kastler, *Move Beyond AIS for Maritime Domain Awareness*, U.S. NAVAL INST.: PROCEEDINGS (Sep. 2025), https://www.usni.org/magazines/proceedings/2025/september/move-beyond-ais-maritime-domain-awareness [https://perma.cc/W9AH-6W96].

[48] *See* Kevin Frazier, *Policy Proposals for the United States to Protect the Undersea Cable System*, 13 CASE W. RES. J.L. TECH. & INTERNET 1, 30–32 (2022) (identifying the high number of undersea cables across two coasts as a barrier to the United States adopting cable protection zones).

[49] *See* NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, STRATEGIC IMPORTANCE OF, AND DEPENDENCE ON, UNDERSEA CABLES 3 (2019) [hereinafter NATO REPORT], https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf [https://perma.cc/GVQ3-2UUS] (warning that terrorists are most likely to attack cables near cable landing stations).

[50] CAMINO KAVANAGH, UNITED NATIONS INST. FOR DISARMAMENT RSCH., WADING MURKY WATERS: SUBSEA COMMUNICATIONS CABLES AND RESPONSIBLE STATE BEHAVIOR 12 (2023), https://unidir.org/wp-content/uploads/2023/05/UNIDIR_Wading_Murky_Waters_Subsea_Communications_Cables_Responsible_State_Behaviour.pdf [https://perma.cc/7ZWA-XJCT]; James Griffiths, *The Global Internet Is Powered by Vast Undersea Cables. But They're Vulnerable.*, CNN (July 26, 2019, at 07:30 ET), https://www.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk [https://perma.cc/A9GM-X4FR].

[51] NATO REPORT, *supra* note 49, at 3; Will Oremus, *The Global Internet Is Being Attacked by Sharks, Google Confirms*, SLATE (Aug. 15, 2014, at 15:23 ET),

use has since spread.[52] New materials may soon promise even greater protection while not unduly burdening operators with the cost and operational difficulties of coiling, then unspooling cables as they're laid on the seafloor.[53] The FCC should expect that operators are continuously studying the availability of superior armoring and justifying the extent to which they do or do not use it.

Second, operators can bury cables at a greater depth and further from the coast. As it stands, the norm is that cables lie on the surface when at a depth of 100 meters or more.[54] This means that in some deepwater ports and high-traffic areas cables may be especially susceptible to sabotage.[55] Operators could additionally be obligated to at least consider the need to use mattress coverings around the cable and assess the placement of nearby rocks, which may shift due to currents.[56]

Third, operators can adhere to minimum separation standards to distance their cables from others. Additional spacing between cables can reduce the odds of a single incident causing numerous breaks. By way of example, in 2008, a single ship damaged six cables by dragging its anchor along the seafloor.[57] Some degree of spacing can make it less likely that one net, anchor, rock, or UUV can break several cables at once.

Fourth, if Congress creates cable protection zones, operators can lay cables in those zones to ease the task of monitoring threats to

---

https://slate.com/technology/2014/08/shark-attacks-threaten-google-s-undersea-internet-cables-video.html [https://perma.cc/4FMN-C5QP].

[52] Griffiths, *supra* note 50.

[53] *See* Darren Orf, *Scientists Created a Bulletproof Material 3 Times Stronger Than Kevlar—It's Already Breaking Records*, POPULAR MECH. (Nov. 11, 2025, at 08:00 ET), https://www.popularmechanics.com/science/a69268884/carbon-nanotube-kevlar/ [https://perma.cc/8387-S97F].

[54] Alex Botting & Inés Jordan-Zoob, *How the US and Its Partners Can Ensure the World's Data Super-Highways Remain Reliable, Secure, Open & Free*, WILSON CTR. (July 15, 2024), https://www.wilsoncenter.org/article/how-us-and-its-partners-can-ensure-worlds-data-super-highways-remain-reliable-secure-open [https://perma.cc/T4TP-MK68].

[55] *Id.*

[56] *Subsea Cables: How Vulnerable Are They and Can We Protect Them?*, JOINT RSCH. CTR., EUR. COMM'N (Aug. 8, 2025), https://joint-research-centre.ec.europa.eu/jrc-explains/subsea-cables-how-vulnerable-are-they-and-can-we-protect-them_en [https://perma.cc/QR9A-XFF2].

[57] *Damage to Submarine Cables from Dragged Anchors*, *supra* note 13.

cables. As the requisite authorities closely monitor these specific areas, they can quickly mobilize the forces necessary to stop a bad actor from "lingering" in that zone as that actor attempts to break several cables in quick succession. Each of these measures will frustrate efforts by bad actors to cause significant and prolonged outages. Operators that opt not to adhere to these defensive measures should again face heightened licensing fees.

V. DIMINISHING THE DAMAGE FROM A SUCCESSFUL ATTACK

In the event that a bad actor manages to break a cable or, in a worst-case scenario, several cables, deterrence calls for policies that ensure network redundancy and rapid repair times. Put differently, adversaries will have less interest in attacking cables if traffic can easily be routed through other cables and damaged cables can be restored in days rather than weeks or months. A case study makes this point clear. When a series of minor accidents caused damage to cables off of Côte d'Ivoire, many Internet users across Africa experienced diminished service.[58] Comparatively, when two cables broke in the Baltic Sea, users experienced few to no issues because of the availability of alternative routes for Internet traffic.[59] That is precisely why redundancy is a key part of a robust undersea cable system.[60]

A redundant undersea cable system includes a number of cables being laid along diverse routes. Congress should study various financial levers to support ongoing cable building both by the United States and its allies, especially in regions that will see many existing cables retired in the coming years. A survey of industry stakeholders suggests that more than 800,000 kilometers of cables will be retired by 2040.[61] As cables reach the end of their operational or economic

---

[58] Paula Gilbert, *Multiple Cable Failures Impact Africa's Internet*, CONNECTING AFR. (Mar. 15, 2024), https://www.connectingafrica.com/connectivity/multiple-cable-failures-impact-africa-s-internet [https://perma.cc/LQ55-SAUM].

[59] David Belson, *Resilient Internet Connectivity in Europe Mitigates Impact from Multiple Cable Cuts*, CLOUDFLARE (Nov. 20, 2024), https://blog.cloudflare.com/resilient-internet-connectivity-baltic-cable-cuts/ [https://perma.cc/FRS3-HE73].

[60] INSIKT GRP., *supra* note 7, at 1.

[61] CONSTABLE, BURDETTE & MAULDIN, *supra* note 6, at 2.

lives, the United States must pay attention to whether our allies are at a heightened risk of prolonged Internet outages resulting from only a few breaks.[62]

While hyperscalers are racing ahead with their own cable projects, the United States has an interest in ensuring redundancy across the entire system.[63] If Google, Amazon, and other hyperscalers do not see an economic case for filling in gaps in the undersea cable system, it is unlikely that other private actors will fill the void. Cable laying is a gamble. Only about half of announced undersea cable projects are completed.[64] An increasingly bifurcated and concentrated supply chain is only making such projects costlier.[65] For all those reasons, it is pivotal that allies look to the United States and not China to increase their own cable connections.

Most importantly, the United States must ensure that any successful disruptions to a cable or cables are short-lived. This is yet another cost-intensive and logistically difficult task. Average repair times have varied over the last few years—taking nearly three months in 2022 (seventy-eight days) while falling to about a month (thirty-two days) in 2025.[66] As the number of cables increases over the next decade[67] and the number of cable repair ships in need of replacement surges,[68] a betting man would like the odds of the average repair time increasing (i.e., expect repair times to rise). This will be especially true if a repair is required during a geopolitical conflict. One industry observer expected that a cable repair ship would demand a military escort prior to sailing to the repair point.[69]

---

[62] *See, e.g.*, EUR. COMM'N, COMMISSION RECOMMENDATION ON SECURE AND RESILIENT SUBMARINE CABLE INFRASTRUCTURES 2 (Feb. 26, 2024), https://ec.europa.eu/newsroom/dae/redirection/document/102534 [https://perma.cc/59XB-BVGJ] (warning that some members of the EU may already be in such a position).

[63] *See generally* KANG & JACOB, *supra* note 4, at 6–7 (estimating that hyperscalers such as Google, Meta, Microsoft, and Amazon have had at least some stake in nearly twenty-five percent of all undersea cable projects that launched between 2019 and 2023).

[64] SUBMARINE TELECOMS F., INC., SUBMARINE TELECOMS INDUSTRY REPORT 2023–2024, at 137 (2023), https://issuu.com/subtelforum/docs/submarine_telecoms_industry_report_issue_12 [https://perma.cc/ZBF7-HJNX].

[65] KANG & JACOB, *supra* note 4, at 10–12.

[66] INDUSTRY REPORT 2025–2026, *supra* note 14, at 100.

[67] CONSTABLE, BURDETTE & MAULDIN, *supra* note 6, at 47.

[68] *Id.* at 61.

[69] UK REPORT, *supra* note 15, at 24.

Congress should swiftly pass legislation like the Neptune Act that aims to bolster the number of cable repair ships.[70] The number of cable repairs is forecast to reach 287 by 2040.[71] Our cable operators should not have Chinese ships on speed dial to patch cables carrying our sensitive communications. Nor should American cable providers expect cable repair ships flying another nation's flag to prioritize repairs to American cables over their own.[72] This is and must be a problem solved by American ships. We are woefully behind on this front.

Minimally, Congress should amend the cable landing license to mandate that operators have at least a ten-year contract with a cable repair provider. This shift would address the financial uncertainty that often prevents cable repair ship owners from further investing in their fleets.

CONCLUSION

The United States is entering an era in which artificial intelligence will amplify every facet of national power—from scientific research and economic productivity to military readiness and diplomatic leverage.[73] But AI's promise is only as strong as the physical infrastructure that undergirds it. Undersea cables are not a peripheral issue in the AI age. Instead, Congress must regard the undersea cable system as a foundational part of the emerging global economy.[74] If these cables are compromised, our most advanced AI labs, high-performance computing clusters, and data-rich enterprises will be unable to operate at the scale that global leadership demands.[75]

---

[70] *See Congressman Max Miller Introduces NEPTUNE Act to Protect America's Critical Infrastructure*, MAX MILLER: DEF. & FOREIGN RELS. (July 25, 2025), https://maxmiller.house.gov/posts/congressman-max-miller-introduces-neptune-act-to-protect-americas-critical-infrastructure [https://perma.cc/J5Y3-R97J] [hereinafter *NEPTUNE Act*].

[71] CONSTABLE, BURDETTE & MAULDIN, *supra* note 6, at 50.

[72] *See* UK REPORT, *supra* note 15, at 25 (expecting French cable repair ships to respond to cables of French significance over cables of importance to the UK).

[73] *See, e.g.*, Tan, *supra* note 2 (projecting economic impacts of $72 billion in 2026 from Meta's AI investments alone).

[74] *See NEPTUNE Act*, *supra* note 70 (pushing Congress to enhance "national security by protecting vital undersea communications infrastructure").

[75] *See* discussion *supra* Part V.

Congress must therefore treat cable resilience not as a niche maritime concern but as a foundational pillar of American competitiveness.[76]

Though Congress should move forward with a "sea shot" over the long term, a focus on deterrence in the short run can collectively reshape the incentives of adversaries and limit the consequences of disruptions. Moreover, as AI systems become more central to real-time intelligence analysis, financial markets, precision agriculture, disaster response, and critical infrastructure management, even brief outages will impose cascading harms.[77] A cable system built for the pre-AI era—an era of slower data flows, fewer real-time applications, and limited global compute—cannot meet the demands we now face.[78] Policymakers must recognize that strengthening undersea infrastructure is not just about preventing sabotage; it is about ensuring that the nation can fully leverage AI to enhance the well-being and security of every American.[79]

Ultimately, Congress has a rare opportunity to act before a crisis forces its hand. The investments and policy changes proposed here will not only strengthen our undersea cable network but also secure the connective tissue of the AI economy for decades to come. With deliberate action—guided by deterrence, informed by evidence, and executed with urgency—the United States can ensure that its cables, like its AI ambitions, are resilient, adaptive, and firmly under American control.

---

[76] *See* discussion *supra* Part V.
[77] *See supra* text accompanying notes 1–11.
[78] *See supra* text accompanying notes 1–11.
[79] *See* discussion *supra* Part V.