美国在海底光缆领域谋取地缘竞争优势的动向及影响[1]

储召锋

【内容提要】海底光缆网络作为数字经济的“水下生命线”，承载着全球99%的洲际通信和数据流量，是世界各国参与全球经济社会活动的基石和载体。近年来，美国通过政策立法、技术管控、联盟构建等多重手段推动海底光缆网络泛安全化，并借机谋取该领域的地缘竞争优势。美国谋取海底光缆领域地缘竞争优势源于数字霸权维护、地缘竞争加剧、技术脆弱性凸显与国内利益协同的多重逻辑驱动，其以“话语实践＋规制壁垒＋公私合作＋联盟围堵”为核心的实践路径，既重塑全球海底光缆治理格局，又引发地缘分裂与数字治理碎片化风险，最终可能反噬美国自身的数字利益与战略信誉。面对美国谋取海底光缆领域地缘竞争优势带来的多重挑战，中国需要做出系统性回应，并推动构建“安全与效率平衡”的治理框架。

【关 键 词】美国政府　海底光缆　泛安全化　地缘竞争　出口管制　数字霸权

【作者简介】储召锋，国防科技大学外国语学院副教授、硕士生导师，中国国际战略学会特约研究员。

【中图分类号】D815

【文献标识码】A

【文章编号】1006-6241（2026）02-0071-26

[1] 本文系国家社科基金重点项目（项目编号：2024-SKJJ-B-102）和有关科研基金项目（项目编号：25-JSLLKY-007）的阶段性成果。作者感谢《和平与发展》匿名评审专家及编辑部对本文提出的宝贵修改意见，文中错漏概由本人负责。

在数字全球化时代，海底光缆（以下简称海缆）已超越传统通信基础设施范畴，成为支撑互联网、5G、云计算、人工智能及跨境金融交易的核心命脉。截至目前，全球运营及在建的跨洋海缆超600多条，总长逾150万公里，承载着全球99%的洲际数据流量[1]，日均传输超10万亿美元的跨境金融数据[2]，其稳定性直接关联全球经济与各国数字主权安全。随着美国推动所谓“大国竞争战略”向深海与数字领域延伸，其对海缆网络问题进行泛安全化操弄的趋势日益明显。自2019年华为被列入“实体清单”以来，美国持续在海缆领域对中国产业链进行系统打压。

2022年“北溪”天然气管道破坏事件发生后，美国作为全球海缆网络的主导者，将消除深海基础设施的脆弱性设为首要议程[3]，加速推进海缆领域的“脱钩断链”进程。2024年12月，美国国土安全部发布《参与海缆安全与韧性优先事项》白皮书，明确将海缆纳入“关键基础设施保护”核心清单。[4]特朗普2.0时代开启后，美国当局显著加大海缆领域的定规立法力度，强化海缆管控措施。2025年2月，白宫发布《“美国优先”投资政策》总统备忘录，要求美国商务部、联邦通信委员会（FCC）、司法部、“通信服务业外国参与审查委员会”（简称“电信小组”，Team Telecom）收紧对中资项目的国家安全审查。[5]同年8月，FCC又通过海缆登陆新规，对来自外国对手的海缆

[1]“Submarine Cable Frequently Asked Questions,” TeleGeography, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

[2]“FCC Votes to Speed Submarine Cable Buildout and Security,” Inside Towers, August 11, 2025, https://insidetowers.com/fcc-votes-to-speed-submarine-cable-buildout-and-security/.

[3] Bueger Christian, Tobias Libetrau, “Critical Maritime Infrastructure Protection: What’s the Trouble?” *Marine Policy,* Vol.155, November 2023.

[4] U.S. Department of Homeland Security, *Priorities for DHS Engagement on Subsea Cable Security & Resilience,* Washington D.C., December 18, 2024, https://www.dhs.gov/sites/default/files/publications/24_12_18-dhs-subsea-cable-security-whitepaper.pdf.

[5] The White House, *National Security Presidential Memorandum on America First Investment Policy,* February 21, 2025, https://www.whitehouse.gov/presidential-actions/national-security-presidential-memorandum-america-first-investment-policy/.

项目申请实施“推定否决”，实际禁用中国、俄罗斯的海缆设备和技术。[1]美国 2026 财年《国防授权法案》专门增列海缆附加条款，禁止联邦资金采购中国海缆及核心部件，要求国防部提交全球海缆安全报告，追加海缆安防经费。[2] 2026 年 2 月，美方以“蓄意授权和支持破坏关键电信基础设施、损害西半球地区安全”为由，对参与推进中企海缆项目的 3 名智利官员实施签证限制，并施压智利政府放弃与中企的合作。[3]美国过度泛化“国家安全”概念，持续加码海缆管控的种种举措，不仅深刻重塑全球海缆建设布局与技术标准，更推动数字时代地缘竞争逻辑变迁。因此，系统解析美国在海缆领域地缘竞争新态势及其影响，对于理解全球数字基础设施治理变革及研判相关地缘政治走向具有重要的理论与现实意义。

一、全球海缆网络的发展格局及主要属性

19 世纪中期，首条海底电缆成功铺设并投入使用，开启了海底通信的新纪元。早期海底电缆是铜质缆线，仅能传输电报信号。经过技术迭代，如今海底电缆已发展为高速光纤网络，成为维系现代社会运转的“信息大动脉”。随着大数据时代对于数字需求的持续增长，建设一个安全、包容且稳定的海缆基础设施体系愈发重要。全球海缆网络主要分布在跨大西洋、跨太平洋及亚欧海域，其中东亚、欧洲与北美是海缆连接密度最高的区域，新加坡、中国香港、日本及美国东海岸构成跨太平洋海缆网络的关键节点。

---

[1] Federal Communications Commission, *Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks,* August 13, 2025，https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf.

[2] U.S. Congress, *National Defense Authorization Act for Fiscal Year 2026,* https://www.congress.gov/119/bills/hr2670/BILLS-119hr2670enr.pdf.

[3] U.S. Department of State, “Visa Restrictions on Chilean Nationals Undermining Regional Security,” February 20, 2026, https://www.state.gov/releases/office-of-the-spokesperson/2026/02/visa-restrictions-on-chilean-nationals-undermining-regional-security.

全球海缆网络长期由私营企业主导运营，市场曾长期被西方企业垄断。近年来，中国海缆企业的崛起势头明显。根据2024年8月美国智库数据，美国海底电子通信（SubCom）、法国阿尔卡特（ASN）和日本电气（NEC）共同占据全球海缆87%的市场份额，中国华海通信（亨通光电子公司旗下子公司）占据11%的市场份额，这四家公司形成全球海缆产业的“四强格局”。[1]美西方凭借技术先发优势和地缘政治联盟，实际控制着全球海缆网络的关键节点和路由选择权；中国虽实现了全产业链自主可控能力与亚太—亚非欧的主导布局，但在跨大西洋/跨太平洋核心路由、登陆节点控制权、西方市场准入与国际话语权上仍处于明显劣势地位。

海缆行业发展前景广阔，既源于全球数字经济蓬勃发展带动国际带宽需求快速攀升，也得益于未来10年将有大量老旧海缆退役带来的更新换代窗口期。受跨境数据、云计算、5G和人工智能等需求驱动，海缆行业进入快速发展阶段，全球投资从2015年的8亿美元增至2025年的97亿美元，累计投资额超450亿美元，现有60余个新项目处于在建或收尾阶段。[2]未来5年，跨太平洋海缆占比将从14%升至近25%，美洲地区由16%降至7%，极地地区从不足0.5%提升至5%。[3]当前海缆投资主体已由传统电信运营商转向大型云服务与内容提供商，他们通过自建自营海缆网络，确保对数据传输的控制权。谷歌、Meta、微软、亚马逊四大云服务商占据全球近75%的带宽需求，在跨大西洋、跨太平洋、亚洲内部三大核心洲际路由上占比超80%。[4]截至2025年底，谷歌已投资

[1] Daniel F. Runde, Erin L. Murphy, Thomas Bryja, “Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition,” CSIS, August 16, 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

[2] ITU, *Global Connectivity Report 2025,* https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2025/, p.58.

[3] SubTel Forum, *SubTel Forum Almanac,* June 2025, https://subtelforum.com/submarine-cable-almanac/.

[4] TeleGeography, *State of the Network 2026,* https://www2.telegeography.com/download-state-of-the-network.

33 条海缆系统，Meta 则投资了 18 条。[1]

海缆网络具有四重属性：一是物理和数据传输安全的脆弱性。海缆暴露于海底且位置公开，实体设施常年面临暴露性威胁。统计显示，全球年均发生 150 ~ 200 次海缆破坏事件，其中约 50% 由捕鱼活动造成，20% 由抛锚导致，其余由人类工程活动及地震等自然现象所致。[2] 此外，海缆网络还面临来自敌对行为的威胁，包括非法截获、复制或转移敏感数据等恶意窃取行为。[3] 其中，窃听海缆存在三种可行方式：在海缆的生产制造环节预置数据采集后门；通过渗透接入海缆的关键接口节点实现数据窃取；在深海环境中直接进行窃听。[4]

二是技术垄断性。海底环境复杂、地质灾害多发，对海缆本体及中继器、分支器等关键设备技术要求苛刻，海缆工程也因此属于技术难度极高的大型基础设施项目。当前高端电缆的制造、铺设与维修技术集中掌握在美、法、中、挪威等少数国家手中，核心设备的供应链安全直接关系海缆建设进度和运营韧性。需要指出的是，受维修技术与设备的稀缺性制约，海缆维修工作一直面临严峻挑战，而且这种挑战未来几年将有增无减。因为一方面，在全球现有 60 艘海缆维修船只中 47% 的船龄已超 20 年，将于 2040 年前集中退役；而另一方面，海缆需求量正在急剧增长，预计 2026—2040 年间，太平洋及北大西洋主要海域新增海缆的

[1] TeleGeography, *State of the Network 2025,* https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2025.pdf.

[2] John Arquilla, "Securing the Undersea Cable Network," Hoover Institution, March 23, 2023, https://www.hoover.org/research/securing-undersea-cable-network.

[3] Justin Sherman, "Cyber Defense across the Ocean Floor: The Geopolitics of Submarine Cable Security," Atlantic Council, September 13, 2021, https://www.atlanticcouncil.org/in-depth-researchreports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/.

[4] Nadia Schadlow, Brayden Helwig, "Protecting Undersea Cables must be Made a National Security Priority," Defense News, July 2, 2020, https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/.

长度将达160万公里，供需矛盾将进一步凸显。[1]

三是司法管辖模糊性。海缆网络跨越公海与专属经济区（EEZ）这一世界上最大的法律灰色地带，穿越多个司法管辖区，常登陆于法律框架各异的国家，使其建设和运营面临独特的地缘政治与法律风险。目前尚缺乏具有强制力的相关国际执法机构，《联合国海洋法公约》以及国际电信联盟（ITU）、国际电缆保护委员会（ICPC）等机构发布的规则和标准多是指导性文件，因而对于海缆的司法管辖主要依赖各国国内立法。这导致沿海国与过境国之间法规不协调、协作机制缺失，既拖延海缆应急修复，也推高了整体建设与运维成本。

四是战略关联性。海缆现被广泛视为一种关键的战略基础设施。海缆布局与全球数字权力直接挂钩，控制关键海缆路由即可影响区域数据流动与信息话语权。数字霸权是美国全球霸权的重要支柱，而海缆网络是其关键物理支撑。长期以来，美国依托AT&T、Meta、谷歌、微软等私营企业主导全球海缆布局，它们参与建设的电缆系统覆盖全球主要海洋航线，掌控近75%的国际数据传输容量。近年来，随着中国海缆产业快速崛起，美国认为对其形成了“战略挑战”。根据国内专业咨询平台智研咨询的数据，截至2025年，中国企业占据全球海缆制造市场35%的份额，其中亨通光电、中天科技等龙头企业占据28%以上份额，主导中低端市场并在高端深海光缆领域实现技术突破，具备5000米级海缆敷设与超低损耗光纤材料的自主生产能力。[2]

二、美国谋取海缆领域地缘竞争优势的动因

为配合其大国竞争战略布局，美国以其海缆网络安全正面临“日益严

[1] ITU, *Global Connectivity Report 2025*, https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2025/, p.60.

[2]《2025-2031年中国海底电缆行业市场发展形势及投资机会研判报告》，智研咨询网，2025年10月16日，https://www.chyxx.com/industry/1236277.html。

峻的挑战与威胁”为由，将原本作为商业属性的海缆产业泛化为“国家安全”议题加以审查和管控，把正常的商业合作渲染为安全威胁风险，以借此打压竞争对手、巩固自身在全球海缆领域的主导地位。其行为背后受到多重逻辑驱使。

（一）地缘竞争逻辑：维护自身数字霸权

在当今数字时代，获取数据并确保其安全正在成为大国战略竞争的核心维度。美国为巩固并拓展其在全球数字格局中的竞争优势，着力谋求数字霸权，并将争夺海缆控制权作为维系自身数字霸权的重要战略抓手。

冷战后，美国曾在海缆领域长期保持技术和市场的主导地位。而近十余年来，中国在数字基建领域突飞猛进，打破了美国的垄断格局。中国政府于2017年提出建设“数字丝绸之路”，鼓励本国企业在全球通信基础设施中扮演更重要角色。此后，以华海通信、中天科技、亨通海洋等为代表的中国海缆企业迅速崛起，在深海海缆制造与超大容量数据传输上实现技术突破。美国将中国在海缆领域的产业突破解读为“数字地缘扩张”，指责中国通过参与“数字丝绸之路”相关电缆项目（如中老泰跨境光缆、中巴经济走廊海缆）建设“平行数字网络”的做法冲击美国主导的全球数字秩序，并将正常的数字产业竞争建构为“国家安全威胁”，从而为其在海缆领域打压中国提供核心叙事。例如，FCC主席布伦丹·卡尔（Brendan Carr）在2025年8月的海缆新规发布会上公开声称，“中国及其他对手国家正越来越多地以海缆为目标，窃取数据、开展间谍活动、破坏关键基础设施。我们必须采取行动保护这一全球互联网重要支柱”。[1]

除了中国，美国也将俄罗斯视为对其数字霸权的重要威胁。2015年以来，美西方媒体多次报道俄罗斯特种潜艇在大西洋海底侦察欧美海缆；俄罗斯被指积极研发海底侦察与破坏能力，如俄深海研究总局在发展能够监听或

[1] Federal Communications Commission, “Carr Statement: FCC Acts to Accelerate Submarine Cable Buildout & Security,” August 13, 2025, https://www.fcc.gov/commissioners/carr/news-releases/2025/undersea-cable-security.

破坏海缆的潜航器等。[1] 美国担忧在未来冲突中俄罗斯可能利用这种不对称手段切断西方跨洋通信系统。

（二）安全脆弱性逻辑：对技术与物理风险过度反应

海缆作为网络空间的关键物理载体，美国认为其“时刻面临双重风险”。一方面是网络窃听与数据截获威胁。美国深谙窃听海缆之道，早在20世纪70年代，美国海军便在鄂霍次克海实施窃听苏联海底通讯电缆的“常春藤之铃”（Operation Ivy Bell）行动，窃取了大量有关苏联核潜艇和弹道导弹技术的情报。[2] 据美国中情局前雇员爱德华·斯诺登（Edward Snowden）透露，美国国家安全局实施的“上游计划”（Upstream）从海缆中复制了海量数据，堪称该局大规模监控系统中最具侵入性的项目。[3] 然而美国却以己度人、“贼喊捉贼”，认为他国也会同样行事。美国国土安全部评估指出，现有海缆的加密技术普及率不足40%，且多数依赖国际通用标准，因而存在“后门风险”。

另一方面是物理破坏与系统瘫痪威胁。在物理安全层面，全球电缆故障事件年均增长8%，其中人为破坏占比达35%。[4] 自2023年以来，波罗的海发生了至少6起海缆遭破坏事件，已造成11条海缆被破坏。[5] 2024年初，红海海域多条亚欧通信光缆疑遭武装破坏。[6] 尽管相关事件尚无证据指

[1] Colin Wall, Pierre Marcos, “Invisible and Vital: Undersea Cables and Transatlantic Security,” CSIS, June 11, 2021, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security.

[2] Sherry Sontag, Christopher Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage,* New York: Harper Collins, 2000.

[3] Edward Snowden, *Permanent Record, London: Macmillan,* 2019, pp.222-225.

[4] International Cable Protection Committee, *Media Enquiries & Frequently Asked Questions,* May 16, 2025, https://iscpc.org/news/media-enquiries/.

[5] Marianna Satta, “The Silent Front: Cable Crisis in the Baltic Sea,” Atlas Institute for International Affairs, April 12, 2026, https://atlasinstitute.org/the-silent-front-cable-crisis-in-the-baltic-sea/.

[6] Olivia Solon, Mohammed Hatem, “Red Sea Cable Cuts Disrupt Global Internet, Houthis Deny Blame,” Reuters, March 6, 2024, https://www.reuters.com/technology/red-sea-cable-cuts-disrupt-global-internet-houthis-deny-blame-2024-03-06/.

向主权国家，美西方战略界却一直对此疑神疑鬼，甚至不乏栽赃嫌疑。美国认为其加勒比地区的海缆网络邻近委内瑞拉、古巴等地缘博弈热点区域，易受海盗破坏与地区冲突波及。更重要的是，由于美国在电缆维修能力上存在短板，谷歌、Meta 等公司的海缆维修任务依靠中国的中英海底系统有限公司等来完成，引发美国对海缆安全的进一步担忧。综上，对于技术与物理脆弱性的过度焦虑，是促成美国将海缆产业与国家安全深度绑定，并借机谋取地缘竞争优势的又一诱因。

（三）经济利益逻辑：保障数字经济核心资产

海缆网络是美国数字经济的“核心生产资料”，直接关联互联网、金融、人工智能等优势产业的发展。美国战略与国际研究中心（CSIS）2022 年 4 月的报告指出，美国 70% 的跨境业务依赖海缆网络传输，海缆支撑着美国 5200 亿美元规模的数字出口业务，每年对美国经济的贡献度高达 1690 亿美元。[1] 根据 2026 年 2 月的数据统计，纽约清算所银行同业支付系统（CHIPS）每天通过海缆网络至少与 40 多个国家和地区处理超过 1.9 万亿美元的金融交易，其报文与清算指令完全依赖海缆实现全球低时延传输，使海缆成为美元跨境清算的物理基石。[2] 随着大数据、云计算和人工智能技术的蓬勃发展，海缆网络支撑全球金融合作与经济稳定运行的作用将持续攀升。美国通过泛安全化操弄谋取海缆领域地缘竞争优势的主要考量在于对数字经济核心资产实施所谓“保护机制”：通过限制外国企业参与，确保本土企业对电缆资源的垄断，维持自身在云计算与数据服务领域的定价权；同时，通过强制实施美国技术标准（如加密协议、硬件规范等），带动国内半导体和通信设备产业的发展。

[1] Matthew Goodman, Matthew Wayland, “Securing Asia’s Subsea Network: U.S. Interests and Strategic,” CSIS, April 5, 2022, https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options.

[2] “Clearing and Settling $1.9 Trillion in Domestic and International Payments each Business Day,” February 20, 2026, https://www.theclearinghouse.org/payment-systems/chips.

（四）国内协同逻辑：契合政府与私营部门的共同利益

私营企业作为海缆铺设、运维及技术研发的核心主体，掌握着全球海缆路由布局、设备制造、数据传输等关键资源。以美国国家安全与情报机构为核心的政府部门则依托国家安全授权、情报能力与战略规划，为私营企业提供政策支持与安全指导，双方形成互补共生的合作关系。基于此，《参与海缆安全与韧性优先事项》白皮书亦明确提出，要优先改善在海缆领域的公私合作关系。[1]

一方面，美国海缆产业高度集中，SubCom、谷歌、AT&T 等 6 家企业占据美国国内 90% 的市场份额。这些企业既希望借助政府设置的政策壁垒排除外国竞争，也希望以国家安全为名获取财政补贴、监管便利与市场保护，以巩固行业优势。2025 年 8 月 FCC 新规简化了本土海缆企业在海缆铺设、登陆与运营环节的许可流程，将审批周期从 18 个月压缩至 6 个月，同时配套税收减免政策。

另一方面，在情报与数据共享层面，私营企业成为美情报机构获取跨境数据的重要渠道（如棱镜计划、上游计划、伏特台风报告），而情报机构则为私营企业提供威胁预警与安全保障。例如，美国国家安全局作为核心技术主导机构，制定了海缆数据传输的军用级加密标准，强制要求谷歌、Meta 等企业在跨境海缆传输中使用其认证的加密算法并预置安全接口，为监控接入提供便利。[2] 在海缆监控技术研发方面，情报机构与企业联合研制水下无人潜航器、光纤传感器、海底监听阵列等装备，如在阿曼—澳大利亚海缆（OAC）项目中，SubCom 受五角大楼资助，秘密部署连接迪戈加西亚美军基地的监听支线。[3] 与此同时，美国中情局、海军情报局等机构向

[1] DHS, "Priorities for DHS Engagement on Subsea Cable Security & Resilience," December 18, 2024, https://www.dhs.gov/sites/default/files/publications/24_12_18-dhs-subsea-cable-security-whitepaper.pdf.

[2] FCC, "Review of Submarine Cable Landing License Rules—National Security Mandates for Encryption and Backdoor Access," *Federal Register,* Vol.90, No.205, October 27, 2025, https://www.govinfo.gov/content/pkg/FR-2025-10-27/pdf/2025-19658.pdf.

[3] Scot Paltrow, Maurice Taman, John Kemp, "Inside the Subsea Cable Firm Secretly Helping America Take on China," Reuters, July 18, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-subcom/.

企业共享海缆威胁情报，助其提前预判水下破坏风险并制定应急响应预案，以减少海缆中断带来的经济损失。谋取海缆领域地缘优势契合美国政府与私营部门的共同战略目标，必然受到双方的共同支持。

三、美国谋取海缆领域地缘竞争优势的实施路径

美国主要通过对海缆议题进行泛安全化操弄来谋取该领域的地缘竞争优势，借助多管齐下式的话语叙事与滥用国家公权力实践两条路径协同推进。首先是通过政府官员、媒体、智库等的公开报告、报道和言论，对海缆网络进行议题框定与“政治化”“泛安全化”构建，赋予其地缘政治属性和“存在性威胁”（existential threat）[1]下的治理优先级；其次是在国家政策响应、军事保护、公私合作以及联盟协同等权力部署领域将海缆网络泛安全化落实为实践层面的政策成果。

（一）话语实践

美国围绕海缆网络构建泛安全化的话语实践，其进程始于21世纪初期的关键基础设施保护浪潮[2]，美国对华战略态势的转变促成了有关海缆安全

[1]“存在性威胁”是所谓“安全化理论”的核心概念，即当某一议题被塑造为影响国家政治、安全的威胁后，政府便可突破常规政策程序，采取“安全导向”的特殊措施（如立法限制、技术封锁等）。参见[英]巴里·布赞、[丹麦]奥利·维夫、[美]迪·怀尔德：《新安全论》，朱宁译，杭州：浙江人民出版社2003年版，第32—37页。

[2] 这一基础设施保护浪潮是21世纪初一系列重大安全事件与制度转向共同建构的结果。“9·11”事件重塑了美国国家安全认知框架，直接推动海缆等通信设施被纳入国家关键基础设施范畴，成为国土安全的重要依托。同期美国海缆产业在互联网泡沫破裂后出现大规模重组与资本格局调整，进一步强化了“海缆属于国家战略资产”的政治叙事。2003年《国家关键基础设施与重要资产物理保护战略》的出台，从顶层设计层面确立了海缆设施的“国家安全属性”定位。而2006—2008年多起跨洋海缆中断事件，则被持续用于渲染基础设施脆弱性与外部威胁风险。与此同时，美国国家安全机构依托“上游计划”等项目在全球海缆系统开展大规模数据采集，进一步将海缆安全议题与情报监控、网络安全防护深度绑定。在上述多重事件叠加之下，美国逐步完成对海缆的泛安全化、政治化话语建构，为后续在该领域推行排他性规制与地缘竞争提供了正当性基础。

叙事的进一步升温。随着全球海缆格局重塑与中国企业参与全球海缆项目的程度加深，美国决策者的战略焦虑日益凸显，愈发臆想“潜在的情报窃取和供应链安全隐患”。

1. 政府官方的叙事建构

在美国官方的话语叙事中，俄罗斯和中国被塑造为海缆安全的“威胁来源”。俄罗斯因具备较强的海军和深海技术，被频繁点名称可能对西方的海缆网络发动蓄意破坏。乌克兰危机爆发后，美欧军事领导人更是直言不讳地对俄罗斯在海缆安全方面的威胁发出警告。2023 年 10 月，时任北约秘书长延斯·斯托尔滕贝格（Jens Stoltenberg）就波罗的海海缆受损事件宣称，“深海基础设施是联盟核心关切，俄方相关活动构成混合战威胁；若证实为蓄意攻击，北约将做出坚定回应”。[1]2024 年 11 月，北约官员詹姆斯·阿帕图赖（James Appathurai）在接受媒体专访时声称，“俄罗斯正系统性地实施海底侦察计划，以‘科考船’为掩护，全面测绘北约海缆与能源管线，这是对西方基础设施最严重的威胁”。[2] 此后，北约新任秘书长马克·吕特（Mark Rutte）、盟军转型司令部司令皮埃尔·旺迪耶（Pierre Vandier）等高官相继发声，推动将海缆安全从技术议题升级为混合战核心威胁。[3]

对中国方面，美国将其定位为谋求“全球通信基础设施控制权”的战略竞争者，声称中国企业主导海缆制造、铺设与运维将给美国带来供应链风险，乃至数据窃密、战时通信中断等安全隐患。美国国土安全部官员称，华海通信

[1] “NATO Chief Promises ‘Decisive’ Response if Baltic Sea Pipeline Damage Resulted from Attack,” Courthouse News Service, October 11, 2023, https://www.courthousenews.com/nato-chief-promises-decisive-response-if-baltic-sea-pipeline-damage-resulted-from-attack/.

[2] Murray S., “Russian Attacks on Undersea Cables: Most Serious Threat to Our Infrastructure,” Euronews, November 28, 2024, https://www.euronews.com/2024/11/28/russian-attacks-on-undersea-cables-most-serious-threat-to-our-infrastructure-nato/.

[3] NATO, “NATO Launches ‘Baltic Sentry’ to Increase Critical Infrastructure Security,” January 14, 2025, https://www.nato.int/cps/en/natohq/news_232122.htm; NATO Allied Command Transformation, “Task Force X Baltic and the Future of NATO Maritime Vigilance,” June 18, 2025, https://www.act.nato.int/article/tfxb-future-nato-maritime-vigilance/.

等中国海缆企业凭借成本优势快速拓展市场，已掌控全球近 30% 的新铺设海缆市场与 25% 的海缆维护市场，“使美国的数字供应链安全面临挑战”。[1]2026 年 3 月，美国国会美中经济与安全审查委员会（USCC）主席薛瑞福（Randall Schriver）在听证会上诬称，中国在海缆、海底采矿等领域的巨额投入，将在 2040 年前“对美国水下优势构成实质挑战，威胁国家安全与供应链安全”；中国海缆部署能力可在战时“切断美军全球通信与后勤供应链”。[2] 诸如此类的叙事增强了受众对华的警惕心理，而泛化和滥用“国家安全”概念，则为美国出台限制中国参与海缆建设的政策营造舆论基础。

2. 大众媒体的舆论塑造

作为海缆安全化叙事的关键传导机制，大众媒体在精英话语建构与公众认知之间形成了关键中介作用。2013 年斯诺登曝光美国国安局“上游计划”后，美国主流媒体开始持续聚焦海缆安全议题并散播恐慌情绪。2014 年克里米亚危机爆发后，随着美西方与俄罗斯的对立态势加剧，相关舆论叙事迅速从数据隐私与监控争议转向海底基础设施安全威胁。《纽约时报》在报道俄潜艇在大西洋海缆路由区域的活动时，刻意选取“特工船只”“出没轨迹”等具有谍战色彩的词汇，配合匿名官员发布美军“持续性焦虑”的表述，成功构建出具有即时威胁性的安全情境 [3]；《海军时报》则将一战时期的英德电缆对抗与冷战时期的监听传统进行历史性关联，暗示俄罗斯正在通过复刻“非对称作战”的历史剧本威胁海缆网络安全。[4] 近年来，相关舆论将

[1] Daniel F. Runde et al., “Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition,” CSIS, August 16, 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

[2] Randall Schriver, “China’s Undersea Capabilities and U.S. National Security,” U.S.-China Economic and Security Review Commission, March 2, 2026, https://www.uscc.gov/sites/default/files/2026-03/02_China-Undersea-Capabilitie-and-U.S.-National-Security.pdf.

[3] Sanger E. David, Schmidt Eric, “Russian Ships near Data Cables are Too Close for U.S. Comfort,” *The New York Times,* October 26, 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

[4] Larter David B., “Navy Grapples with Russian Threats to Undersea Cables,” *Navy Times,* October 31, 2015, https://www.navytimes.com/news/your-navy/2015/10/30/navy-grapples-with-russian-threat s-to-undersea-cables.

矛头明显转向美国认定的“最大威胁”中国。例如，2024年5月《华尔街日报》等美媒着力炒作中英海底系统有限公司的海缆维护船只在作业时关闭卫星跟踪系统以“隐藏位置”，构陷该公司在此期间“可能安装窃听设备或从事破坏行为”，从而“威胁美国的商业与军事数据安全”。[1]

整体看，美国主流媒体的话语传播实践与官方叙事相辅相成，官方提供权威信息源和威胁评估，媒体则扮演“助推器”角色，通过大量细节、数据和专家引述使海缆网络安全问题转化为公共议题，将威胁叙事植入公众认知结构，构建“海缆安全等于国家安全”的话语体系，以为相关政策实践铺平道路。

3. 战略界的理论支撑

在近年海缆网络安全议题的兴起过程中，美国智库及战略学者发表的有关报告、论文和“专家意见”提供了所谓的理论支撑。新美国安全中心中国问题专家艾尔莎·卡尼亚（Elsa Kania）撰文臆断，中国在台海周边的海缆布局可使其在战时实施信息封锁，切断台湾与全球的通信渠道，并瘫痪美军在“印太”地区的指挥与情报系统。[2]传统基金会研究员成斌（Dean Cheng）诬指中国海缆网络旨在监控全球数据流动并对西方网络进行渗透，“威胁美国国家安全”，并呼吁美国禁止中企参与美国及其盟友的海缆项目，构建“去中国化”的安全海缆联盟。[3]保卫民主基金会中国问题研究员克雷格·辛格尔顿（Craig Singleton）宣称，中国海缆企业如果主导全球海缆制造与铺设，可能会“将关键基础设施武器化”；美国必须限制中企参与美国

[1] “US Warns Tech Giants: Chinese Vessels may Disrupt Pacific Subsea Cables,” *The Wall Street Journal,* May 19, 2024, https://www.wsj.com/tech/us-warns-tech-giants-chinese-vessels-may-disrupt-pacific-subsea-cables.

[2] Elsa Kania, “Undersea Warfare in the Indo-Pacific: China’s Cable Strategy and U.S. Response,” CNAS, February 10, 2024, https://www.cnas.org/publications/reports/undersea-warfare-in-the-indo-pacific-chinas-cable-strategy-and-u-s-response.

[3] Dean Cheng, “China’s Undersea Cable Ambitions: A Threat to U.S. National Security,” The Heritage Foundation, March 5, 2025, https://www.heritage.org/defense/report/chinas-undersea-cable-ambitions-a-threat-to-us-national-security.

海缆建设，以维护数字基础设施安全。[1]

总之，美国智库及战略学者围绕海缆议题提供的理论支撑主要体现在两个方面：一是他们用“专业分析”证明相关威胁“真实存在”，以减轻公众对海缆安全问题可能被过度夸大的疑虑；二是他们通过参与相关课题的讨论和提出决策建议，引导海缆网络从话语阶段走向实际政策。

（二）政策实践

在对海缆网络议题进行泛安全化话语建构的同时，美国在规制壁垒、军事保护、公私合作以及联盟体系等方面展开了一系列政策响应和实践安排，将海缆产业与国家安全深度绑定，试图巩固自身在海缆领域的主导地位。

1. 打造规制壁垒

当前深海空间的规则相对缺位，各国往往依照本国法律管理所辖区域的海缆。在将海缆议题进行泛安全化操弄过程中，美国通过积极开展立法行动、严格把控海缆登陆的许可审批以及进行出口管制等，规制企业等国际行为主体参与海缆建设与运营的行为。

一是健全安全规制体系。在准入环节，强化外国对手准入限制。为进一步加强技术封锁，2025 年 FCC 新规确立了对外国对手“预设否决”的原则，明确将中国、俄罗斯等国家的相关实体纳入“高风险清单”，对其参与的电缆项目实施“推定拒绝”，仅在“无替代方案且符合国家利益”的情况下才可能让其获批。同时，新规扩大“电信小组”的审查范围，要求其不仅审查企业股权结构，还要披露供应链所有环节的合作方。[2] 在运营环节，增设严苛安全要求，强化全流程管控。《参与海缆安全与韧性优先事项》白

[1] Craig Singleton, “China’s Undersea Cable Dominance and the Threat to U.S. National Security,” Foundation for Defense of Democracies, July 15, 2025, https://www.fdd.org/analysis/2025/07/15/chinas-undersea-cable-dominance-and-the-threat-to-us-national-security.

[2] Federal Communications Commission, *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks,* August 13, 2025, https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf.

皮书强制要求在美国登陆的海缆项目须实行“三重防护”，即物理防护、网络防护、应急防护，同时配合美国政府部门开展安全审查与威胁监测。[1] 美国国土安全部还发布规定，要求 FCC 对违反海缆安全与韧性强制标准、“电信小组”安全审核机制及《海缆登陆许可法案》的企业，依法吊销其海缆登陆许可证，并处以最高 2 亿美元的罚款。[2] 在退出环节，FCC 新规增设“国家安全例外条款”，授权政府可在“紧急情况”下强制接管外国企业参与的海缆项目，以确保关键时期的网络控制权。

二是严格许可审查，实施长臂管辖。美国以国家安全为名，要求任何在美登陆的海缆项目，都必须获得 FCC 颁发的许可证。特朗普在第一任期签发总统行政令，将“电信小组”转变为正式的跨部门电信审查机构，具体负责审查 FCC 提交的每一份申请。此后，“电信小组”推动 FCC 将华为、中兴、中国电信、中国移动等列入“安全威胁实体清单”，主导否决了多项中资企业参与的海缆项目。2025 年 FCC 新规采取“区别对待”的审批逻辑，一方面简化美国本土企业及盟友企业参与的海缆项目审批流程，另一方面却提高涉及“外国对手”或“存在安全风险”项目的审查标准，大幅延长其审批周期。[3]

三是加大技术出口管制力度。美国国会显著加大对海缆技术出口管制的立法力度，主要以推进“海底电缆管制法案”为核心，同时依托《2018 年出口管制改革法案》（ECRA）形成配套管控。“海底电缆管制法案”是美国国会近年推动的最具针对性的海缆技术出口管制专项法案，已于 2025 年

[1] U.S. Department of Homeland Security, “Priorities for DHS Engagement on Subsea Cable Security & Resilience,” 2024, https://www.dhs.gov/sites/default/files/publications/24_12_18-dhs-subsea-cable-security-whitepaper.pdf.

[2] Federal Communications Commission, *FCC-25-49 Report and Order,* https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf.

[3] Federal Communications Commission, *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks,* August 13, 2025, https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf.

9月经众议院通过，后续如果成法，将为出口管制提供明确依据，以阻断“外国对手”对海缆核心技术与设备的获取渠道。《2018年出口管制改革法案》是美国出口管制的核心框架性法案，“海底电缆管制法案”明确要求其战略制定需与该法案政策保持一致，以确保海缆技术出口纳入美国整体出口管制体系。此外，“海底电缆管制法案”还要求美国政府积极推动谋取在海缆相关国际标准制定机构中的领导地位，防范“外国对手”通过标准制定削弱美国出口管制的效果。

2. 制定军事保护策略

鉴于海缆遍布全球公共海域且易遭蓄意破坏，美国军方制定了多层次的保护策略，包括加强海底监视巡逻、提升应急修复能力，以及与盟友展开联合演习等。美国正恢复冷战时期的深海军事部署，加大深海态势感知能力建设。例如，投入数十亿美元重启冷战时期的“综合海底监视系统”（IUSS），通过部署水下卫星[1]、水下传感器以及人工智能等新技术，提升对海缆等深海基础设施的防护能力。[2]为维持海缆运维能力，美军正计划增建海缆铺设与维修船只，以缓解现有船队数量不足、装备老化问题。2025年7月，美国众议院通过“海军加强电信海底网络设备保护法案”（NEPTUNE Act），旨在授权海军新建2艘海缆铺设与维修船，并要求在替代船只具备同等或更优能力前，“宙斯”号海缆作业船不得退役。[3]

2022年“北溪”天然气管道破坏事件凸显了海底基础设施的脆弱性，美国趁机将海缆安全纳入北约议程，推动将其纳入“北约集体安全的重要

[1] 此处“水下卫星”是指以分布式无人潜航器、海底传感器、无人滑翔机为核心的水下自主监视网络，它是美军“综合海底监视系统”升级的核心要件。参见Anna Knight, “U.S. Ocean Surveillance Systems: Land, Sea, Air, and Space,” Grey Dynamics, May 22, 2025, https://greydynamics.com/u-s-ocean-surveillance-systems-land-sea-air-and-space/。

[2] Joe Brock, “Exclusive: U.S. Navy Revives Cold War-era undersea Spy Network to Counter China,” Reuters, September 21, 2023, https://www.reuters.com/investigates/special-report/usa-china-tech-surveillance/.

[3] *H.R. 4625 (119th): Naval Enhancement for Protection of Telecommunications Undersea Network Equipment Act,* GovInfo, July 23, 2025, https://www.govinfo.gov/content/pkg/BILLS-119hr4625ih/pdf/BILLS-119hr4625ih.pdf.

组成部分”。2024 年 2 月，北约国防部长会议通过专项决议，成立“关键海底基础设施网络”，将海缆保护纳入北约集体防御范畴，重点强化波罗的海、北大西洋等关键区域的保护力度。[1] 与此同时，美国与其北约盟友举行多场联合演习，以提升海底基础设施的保护能力。2025 年 1 月，北约启动“波罗的海哨兵”（Baltic Sentry）行动，部署舰艇、无人水下航行器和侦察机等在波罗的海海域开展持续巡逻，以防范潜在对手对海缆和能源管道的破坏行为。[2]2025 年，英国与挪威主导开展系列联合反潜巡逻与海缆保护演习，重点针对俄罗斯潜艇在北大西洋海缆附近的“可疑活动”。[3]2026 年初，英国与挪威再次联合行动，跟踪监测在北大西洋海缆周边活动的俄罗斯潜艇，最终迫使其撤离该区域。[4]

3. 推进公私合作与信息共享

美国谋求海缆领域地缘竞争优势，高度依赖政府与私营部门的利益协同。美国国土安全部通过“关键基础设施伙伴关系咨询委员会”（CIPAC）等机制，吸纳基础设施运营方参与跨部门协作，以确保政策协调与行动一致性。脱胎于冷战时期美国侦察苏联潜艇秘密项目的 SubCom，既是全球主要海缆开发商，也是美国军方独家海缆承包商，如今成为政府机构与私营企业合作的核心枢纽。SubCom 于 2021 年获得美国交通部每年 1000 万美元合同，运营两艘海缆维修船组成的电缆维护船队，为美国全球关键海

[1] Winston Qiu, “NATO Holds First Meeting of Critical Undersea Infrastructure Network,” Submarine Cable Networks, August 14, 2024, https://www.submarinenetworks.com/en/nv/insights/nato-holds-first-meeting-of-critical-undersea-infrastructure-network.

[2] NATO, “NATO launches ‘Baltic Sentry’ to Increase Critical Infrastructure Security,” January 14, 2025, https://www.nato.int/cps/en/natohq/news_232122.htm.

[3] UK Ministry of Defense, “UK and Norway to Operate Together to Counter Russian Undersea Threat through Major New Defense Agreement,” December 4, 2025, https://www.gov.uk/government/news/uk-and-norway-to-operate-together-to-counter-russian-undersea-threat-through-major-new-defence-agreement.

[4] Jill Lawless, “UK and Norway Led a Military Operation to Deter Russian Submarines in the North Atlantic,” The Associated Press, April 9, 2026, https://apnews.com/article/britain-norway-russian-submarines-atlantic-7aa163bc29266504dd1d4c9949aeafde.

缆提供巡检与应急修复服务。[1] 该公司还参与 SEA-ME-WE-6（东南亚—中东—西欧 6 号，2024 年至今）、北极航线（2025 年至今）等海缆项目，持续深化与美国政府的利益绑定，成为美国海缆安全管控的核心依托力量。此外，谷歌、Meta、亚马逊等“超大规模”内容提供商也在政府鼓励支持下，持续加大对跨洋海缆项目的投资力度，2025 年相关投资计划超过 30 亿美元。[2]

值得注意的是，近年人工智能发展对数据流动、数据中心互联的需求急剧扩大，也促使谷歌、Meta、亚马逊等巨头倾向于建设自有海缆网络，以在提升通联效率的同时降低对外部供应商的依赖。它们的参与不仅扩展了海缆网络规模，还通过改进波分复用（WDM）技术以及提高光纤对数容量，推动了光缆技术的进一步发展。[3] 这些项目皆由私营财团主导建设，美国联邦和州政府提供上岸许可、税收及环保等方面的政策保障。

4. 联合盟友开展排他性竞争

一方面，为巩固在全球海缆网络中的主导地位，美国依托多层次联盟体系强化盟友战略协同。拜登政府尤为重视北约、G7、五眼联盟、三海倡议[4] 等机制下的海缆政策协调，并通过美日印澳“四方安全对话”（QUAD）、“全球基础设施和投资伙伴关系”（PGII）、“美印关键与新兴技术倡议”（iCET）等制度性安排，将军事安全与意识形态因素融入数字基建竞

[1] Dan Swinhoe, “US Government Paid for Secret Spur on Oman Australia Cable to Naval base on Diego Garcia Island,” Datacenter Dynamics, July 6, 2023, https://www.datacenterdynamics.com/en/news/us-government-paid-for-secret-spur-on-oman-australia-cable-to-naval-base-on-diego-garcia-island/.

[2] TeleGeography, “Building Tomorrow’s Internet: A 2025 Update on New Cable Investment,” May 15, 2025, https://blog.telegeography.com/building-tomorrows-internet-an-update-on-new-cable-investment.

[3] “Subsea Cable Market Set to Reach US $68.60 Billion by 2033, Driven by Surging Global Bandwidth Demand and Digital Infrastructure Investment,” March 12, 2026, https://lingoexp.com/release/202627250.html.

[4] “三海倡议”即波罗的海、亚得里亚海和黑海倡议，由波兰和克罗地亚两国于 2015 年提出，旨在加强中东欧国家间能源、交通和数字化基础设施间的合作，成员国包括波兰、克罗地亚、保加利亚、捷克、匈牙利等 13 个中东欧国家。美国是其重要战略伙伴。参见《第十届“三海倡议”峰会聚焦基础设施和能源合作》，新华网，2025 年 4 月 30，http://www.xinhuanet.com/world/20250430/21d484d85b7c465a8b737e34e1e8dc8c/c.html。

争，在海缆领域构建起排他性的“技术联盟”。2024 年 7 月，澳大利亚启动印太“电缆连接与韧性中心”，计划在未来四年内向该中心投资超过 1800 万澳元（约合 1180 万美元），支持所谓“印太”地区相关国家制定海缆政策与法规，同时提供技术援助和培训。[1] 与此同时，QUAD 通过持续帮助地区较小国家获得可靠的通信和互联网服务，试图将中国公司排除在承载互联网流量的关键海缆之外。

另一方面，为对中国海缆网络进行物理孤立，美国撮合盟友打造排华海缆新线路。太平洋岛国因其独特的地缘战略价值而成为美国对华战略竞争的重要场域。2021 年，华海通信投标了由世界银行牵头的“东密克罗尼西亚电缆项目”，该项目旨在通过铺设海缆改善瑙鲁、基里巴斯和密克罗尼西亚联邦等太平洋岛国的通信条件。虽然中国企业具备技术与价格双重优势，但由于该电缆将经过关岛，美国联合澳大利亚以安全风险为由向相关岛国及世界银行施压，禁止它们选择中国供应商，最终导致整个招标失败。

新一届特朗普政府虽不如拜登政府那样热衷拼凑“意识形态同盟”，还因意图吞并加拿大和格陵兰岛以及与以色列联手发动对伊朗的军事打击等问题而与诸多盟友的分歧和裂隙加大，但在谋求海缆领域地缘优势这一目标上并未改变。2020 年特朗普第一任时期就将海缆纳入“清洁网络”计划的核心领域，大搞小集团排挤中国企业；其第二任期更关注经济与产业安全，在“美国优先”战略指导下，必然继续逼压盟友配合其打压竞争对手，以维持美国在全球海缆领域的主导权。

四、美国谋取海缆领域地缘竞争优势的影响

美国通过泛安全化操弄和公权力滥用谋取海缆领域地缘竞争优势的行为，对地缘政治关系、全球海缆治理和全球数字经济带来重大冲击，并将

[1] John Tanner, “Australia Launches Centre for Pacific Island Subsea Cable Resilience,” Developing Telecoms, July 30, 2024, https://developingtelecoms.com/telecom-technology/optical-fixed-networks/17077-australia-launches-centre-for-pacific-island-subsea-cable-resilience.html.

引发数字地缘[1]分裂与数字治理碎片化风险，最终可能反噬美国自身的数字利益与战略信誉。

（一）加剧数字地缘格局的分化对立态势

在地缘和技术博弈不断加剧背景下，美国推动海缆网络的政治化、泛安全化进程，不仅反映了其国家安全理念的变化，也体现出基础设施安全化在全球地缘政治层面的外溢效应。美国将国际格局中权力竞逐的维度从传统的军事、政治、经贸领域扩展到数字基础设施领域，将海缆网络转化为地缘竞争的新战场。例如，在“印太”地区，美国主导的“可信电缆网络”与中国参与的“数字丝绸之路”电缆项目形成平行布局：美国推动的“美日澳印”电缆项目（连接关岛、达尔文、新加坡）与中国参与的“中泰老缅”电缆项目，分别依托不同合作机制建设，导致数据传输路径的碎片化态势，削弱了区域数字基础设施的协同发展与数据互联互通。美国恢复深海监视系统、部署水下卫星、建造间谍潜艇等举措带有明显的军事属性，危害他方所建设和运营的海缆网络的安全，可能引发深海军备竞赛。总之，美国滥用国家安全概念在海缆领域推动“脱钩断链”，将加剧数字地缘格局的分化对立态势。

（二）冲击全球海缆治理体系

美国以泛安全化逻辑在海缆领域实施政策操纵，借机推进地缘政治竞争，这一行为对全球海缆治理体系构成了碎片化与意识形态化的双重冲击，违背互联互通、普惠共治的数字全球化发展理念。在治理机制层面，传统的海缆治理以国际电信联盟为核心，遵循“技术中立”“多边协商”“非歧视性”原则，但在美国的联盟构建与单边规制政策影响下，逐渐形成了“多边机制 + 小圈子联盟”的双重治理格局。例如，美国主导的“可信电缆伙

[1]“数字地缘”是一个融合了传统地缘政治逻辑与数字技术、数字基础设施特征的概念，意指地缘政治博弈的焦点从物理疆域（如领土、领海等）延伸到由数据流、数字基础设施和数字技术标准构成的虚拟空间。参见叶成城：《数字地缘政治学：空间特征、资源分布与权力要素》，载《当代世界与社会主义》2025 年第 3 期，第 158—159 页。

伴计划”绕过国际电信联盟自行制定标准与准入规则，导致全球海缆治理出现标准互斥的两套体系，增加了跨国电缆项目的协调成本。在治理理念层面，美国将“安全优先”凌驾于“效率与公平”之上，其对“外国对手”的界定带有强烈意识形态色彩，打破了传统海缆治理中的“非歧视性”原则，从而持续推高数字领域的互信赤字。

在此背景下，中小国家在选择海缆合作伙伴时，不得不在经济利益和政治压力之间做出取舍。例如，一些太平洋岛国在美、澳压力下出于安全考虑，最终放弃与中国公司合作，转而接受更为昂贵的美澳方案，沦为美国地缘博弈的牺牲品。此外，由于美国主导的技术标准门槛较高，发展中国家短期内难以承担合规成本，导致这些地区的互联网普及率提升缓慢，进一步加深了全球数字鸿沟。

（三）拖累全球数字经济发展前景

一方面，美国违背海缆作为市场化商业产品的本质属性，将其异化为对华竞争的地缘工具，将导致行业竞争减弱，推高海缆建设成本。以华海通信为代表的中国海缆企业迅速崛起，打破了美日欧“三足鼎立”的垄断格局。中国企业的加入带来更低的报价和新的商业模式，如前文所述的Sea-Me-We-6项目，华海通信的报价比美国SubCom公司低20%。然而，在美国干预下，该项目最终由SubCom中标，美国政府还通过出口信贷为其提供约6亿美元的低息贷款支持。[1] 美国的排他性举措干扰了市场机制的正常运行，使海缆等基础设施建设成本面临额外的溢价压力，可能直接导致资金资源相对有限的发展中国家的海缆项目延期甚至无法实施，从而阻碍当地的互联网普及和数字经济发展。

另一方面，美国阻挠中美直连海缆项目，损害了全球数据流的合理路径布局。香港凭借地理区位、基础设施和市场优势，曾是美企跨太平洋海

[1] Robert Clark, “US Hardball Drove Chinese Vendor from Huge Cable Project: Reports,” Light Reading, March 27, 2023, https://www.lightreading.com/cable-technology/us-hardball-drove-chinese-vendor-from-huge-cable-project-reports.

缆的首选登陆地。然而，2020 年以来，美国以泛安全化政治理由拒绝新海缆登录香港，否决了至少 4 条原规划连接香港的海缆项目[1]，削弱了香港亚太通信枢纽地位。2025 年 2 月，特朗普签署“美国优先”投资政策备忘录，收紧中国对美关键基础设施投资审查，防范中国借海缆等基础设施“获取敏感数据”“威胁美国国家安全”。[2] 同年，FCC 出台新规，禁止任何包含中国技术或设备的海缆接入美国，彻底阻断中企参与中美直连光缆建设。未来跨境数据流或将呈现“两段式”格局：一段在美国及其盟友的海缆网络内部高速流动，另一段在中国及其伙伴国家的海缆网络内部高速流动，而两者之间仅通过有限节点转接，类似于形成“网络围墙”。美国与中国在海缆领域的博弈加剧，可能引发全球数字基础设施的分裂与脱钩，对全球数字经济与技术创新造成长远损害。

（四）反噬美国自身利益

美国在海缆领域进行的地缘竞争操弄虽在短期内看似维护了本国利益，但长期下去将产生多重反噬效应。一是造成产业成本上升。美国普林斯顿大学《公共和国际事务》杂志分析指出，美国企业的海缆修复严重依赖中国，排除中企本质是损害自身利益的行为，将直接推高海缆的新建与维护成本，使美国企业失去中国市场。[3] 另据美国电信与互联网权威平台报道，Meta 的“非洲数字环”（2Africa）、谷歌的“蓝色拉曼”（Blue-Raman）等重点海缆项目，因美国对中企限制导致企业相关支出同比上升 15%，上述项目也

[1] David Shepardson, “US Agency to Launch Review of Undersea Cables, National Security Risks,” Reuters, October 31, 2024, https://www.reuters.com/technology/us-agency-vote-launch-review-undersea-cable-vulnerabilities-2024-10-31/.

[2] The White House, *National Security Presidential Memorandum on America First Investment Policy,* February 21, 2025, https://www.whitehouse.gov/presidential-actions/national-security-presidential-memorandum-america-first-investment-policy/.

[3] Anna Blue, “Submarine Data Cables: Latest Target of the U.S.-China Rivalry,” *Journal of Public & International Affairs,* September 24, 2024, https://jpia.princeton.edu/news/submarine-data-cables-latest-target-us-china-rivalry.

因成本追加而陷入停滞。[1]

二是导致技术创新停滞。美国通过设置技术规制壁垒、强化安全许可审查、推行违背市场原则的排他性竞争以谋取地缘优势，虽能为本土企业带来短期收益，却使其陷入封闭供应链与低水平竞争环境，长期将显著削弱产业创新动力，最终导致海缆产业效率下滑与技术创新趋缓。为维护所谓国家安全，美国强制本土海缆登陆站采用认证设备并将华为、中兴等列入供应商禁令，对境内运营商实施严格约束。然而在其管辖范围外，多数国家出于经济效益并未跟进此类限制。这使得美国推动海缆网络“脱钩”在供应链层面存在明显的自我削弱隐患，进而制约本土企业对核心技术与关键部件的研发突破。

三是侵蚀联盟内部战略互信基础。美国以“清洁网络”“民主联盟”等名义强推技术壁垒的做法，与数字技术的全球化属性背道而驰。而特朗普第二任期推行极端安全化政策，强制盟友排除中国海缆企业、采用美方技术标准并承担安全成本，引发欧盟、英国、澳大利亚等核心盟友的质疑与不满。欧盟多次明确表态，海缆属于全球性民用基础设施，其建设与运营应恪守市场化原则，并呼吁建立欧盟自主的海缆安全治理框架而非盲从美国。[2] 英国外交部公开反对将海缆安全问题过度政治化，担忧美国推行的“一刀切”排华政策将推高英国海缆项目的建设成本、加剧供应链的单

[1] Dave Ritchie, “Meta’s 2Africa Undersea Cable—the Most Ambitious Internet Project on Earth—Is Stuck in Geopolitical Quicksand,” Web & IT NEWS, March 14, 2026, https://www.webanditnews.com/2026/03/14/metas-2africa-undersea-cable-the-most-ambitious-internet-project-on-earth-is-stuck-in-geopolitical-quicksand/; “Google and Meta Suspend Red Sea Submarine Cable Plans with Some Operators Evaluating Alternative Routes,” *DIGITIMES,* November 19, 2025, https://gb-www.digitimes.com.tw/tech/dt/n/shwnws.asp?PACKAGEID=73980&id=0000738522_M556TEWP1VDPGE3Q6KRTP.

[2] Luigi Scazzieri, *Hedging against Uncertainty: How European Defense is Adapting to Trump 2.0,* European Union Institute for Security Studies, https://www.iss.europa.eu/sites/default/files/2025-10/CP_187_ch1.pdf; European Commission Digital Strategy, *Commission and the High Representative Present Strong Actions to Enhance Security of Submarine Cables,* February 21, 2025, https://digital-strategy.ec.europa.eu/en/news/commission-and-high-representative-present-strong-actions-enhance-security-submarine-cables.

一化风险，同时损害英国与亚太地区的数字联通，拖累“全球英国”战略推进。[1] 澳大利亚同样对美国政策的负面影响表示担忧，认为此类政策可能导致区域海缆项目陷入停滞，主张在保障安全需求与兼顾区域发展利益之间寻求平衡。[2] 在全球经济复苏动能不足、各国财政普遍承压的背景下，海缆联盟成员国更倾向于基于经济理性做出市场化选择，成本收益核算在海缆项目决策中的权重上升，这一趋势也将进一步侵蚀美国与联盟成员之间的战略互信基础。

四是破坏全球通信稳定。海缆多跨公海与专属经济区，应对自然灾害及人为破坏高度依赖国际协作。美国出于地缘竞争目的推行排他性政策，严重冲击多边合作，加剧全球海缆系统脆弱性。同时，国际协作机制弱化也降低了对海缆蓄意破坏行为的预警与溯源能力。2023 年以来，波罗的海频发海缆破坏事件，也门附近多条洲际光缆疑遭袭击，均凸显全球数字基础设施安全风险上升。当一国的安全诉求凌驾于国际合作和各国共同利益之上时，全球通信网络安全必将受到损害。

结 语

美国在海缆领域通过泛安全化操弄推进地缘竞争议程，既折射出数字时代国家安全议题的过度泛化和滥用趋势，也预示着全球数字基础设施治理步入“地缘政治化”的新阶段。美国挑动海缆领域地缘政治竞争，虽然可在短期内获得国内与盟友政治支持，但长期将面临“威胁叙事透支”与“应对机制失效”风险。随着中国技术自主能力的提升与发展中国家

[1] UK Government Foreign, Commonwealth & Development Office, “UK Submarine Cable Security: International Cooperation and Independent Risk Assessment,” April 6, 2025, https://www.gov.uk/government/publications/uk-submarine-cable-security-international-cooperation.

[2] William Jackson, Ryan Robertson, “Pentagon Questions AUKUS Submarine Deal as Costs, Delays Mount,” Straight Arrow News, June 13, 2025, https://san.com/cc/pentagon-questions-aukus-submarine-deal-as-costs-delays-mount/.

对多元合作模式的需求，美国的规制与围堵策略将逐渐失效，而其一系列单边利己操弄所累积的治理成本与地缘政治风险，将使国际社会重新审视“安全优先”的合理性，并对其在海缆领域谋取地缘竞争优势的本质和前景形成更理性的认知。

2025年10月习近平主席在釜山同特朗普总统会晤时强调：“中国的发展振兴同特朗普总统要实现的‘让美国再次伟大’是并行不悖的，中美两国完全可以相互成就、共同繁荣。”[1]这一论述为中美两国妥善处理海缆问题指明了解决思路。作为全球数字基础设施的两大核心参与者，中美若能构建建设性合作框架，不仅能促进技术标准协调与国际规则共建，更有助于增强全球数字供应链的安全韧性与运行效率。基于此，中国应持续敦促美国理性看待中国海缆产业发展与全球数字经济的共生性，摒弃零和博弈思维，停止泛化国家安全概念及将普通议题政治化、工具化甚至武器化的做法，促使美方认清合作共赢是实现海缆网络安全与可持续发展的关键要素。未来十年，全球海缆网络将迎来新旧交替的关键窗口期。为此，中国需提前做好系统性的战略规划与布局，通过持续推进产业技术创新、强化标准规则国际供给、深化多边机制协同等举措，推动构建“安全与效率平衡”的海缆治理框架，从而以更强的产业韧性与更灵活的外交布局，有效化解美国为谋取地缘竞争优势在海缆领域加大对华遏制打压的挑战。

【收稿日期：2025-12-18】
【修回日期：2026-04-23】
（责任编辑：李万胜）

[1]《特写｜“中美两国可以相互成就、共同繁荣”》，新华网，2025年10月30日，http://www.xinhuanet.com/politics/leaders/20251030/0c2af65a5fb54a31902909ae216534f1/c.html。