hinrich foundation

advancing sustainable global trade

APRIL 2024

The new geopolitics of undersea cables

BY ALEX CAPRI
RESEARCH FELLOW, HINRICH FOUNDATION

Contents

Introduction

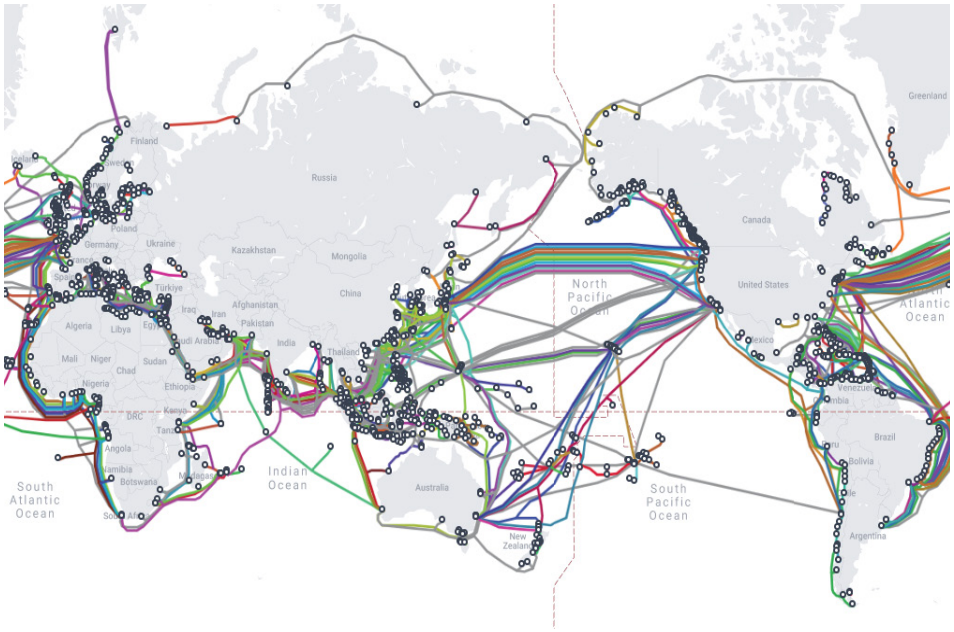
The most densely packed clusters of cables originate and terminate between the United States and Europe, and these same places have major arterials connecting to economic hubs in Asia, namely Japan, China, Taiwan, and about a dozen other places.

Most people are surprised to learn that before information and data in the digital cloud can be accessed, it must first pass through a vast network of undersea cables. Today, close to 99% of the traffic on the internet flows through a sprawling network of fiber optic cables, each around three centimeters in diameter.[1]

There are roughly 575 active cable systems laid across the vast abyssal plains of the world's oceans and under the territorial seas of nations, comprising about 1.4 million kilometers of connectivity. All told, these cables are essential for the daily communications of billions of people and businesses.[2] In 2023, undersea cables carried an estimated US$10 trillion worth of financial transactions every day.[3]

Most of the cables carrying our voice, data, and streaming images lie remarkably exposed on seafloors, on average, about 3,600 meters deep. The longest such underwater linkage, the Asia-America Gateway, runs an incredible 20,000 kilometers and connects Southern California to landing points in Hawaii, Guam, the Philippines, China, Vietnam, Brunei, Malaysia, and Vietnam.

To view a map of the world's undersea cable networks is to understand which countries and commercial hubs command the greatest flows of wealth, knowledge, and power. As such, the most densely packed clusters of cables originate and terminate between the United States (US) and Europe, and these same places have major arterials connecting to economic hubs in Asia, namely Japan, China, Taiwan, and about a dozen other places.



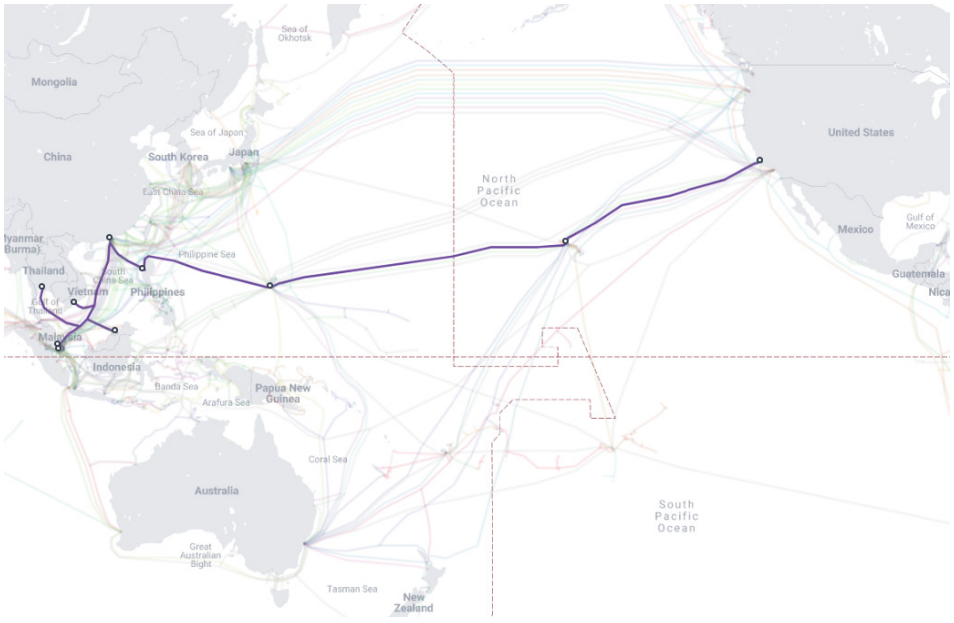
To view a map of the world's undersea cable networks is to understand which countries and commercial hubs command the greatest flows of wealth, knowledge, and power.

Geopolitics, data, and undersea cables

Undersea cables are central to the hybrid Cold War between the US and China. In a geopolitical context, because of their ubiquity, they are far more consequential than 5G wireless network infrastructure and — at least into the foreseeable future — space-based satellite communications. At stake is the motherlode of data that flows through the open internet. This includes transfers to and from the world's data storage centers in the cloud, communications between multinational companies, banking transactions, and even intra-military and governmental data flows.

From a techno-nationalist perspective, whoever excels in manufacturing, laying, and maintaining cable, as well as accessing and defending these undersea cable networks achieves not only economic power, but also gains defense and intelligence-gathering advantages. The potential weaponization of these technologies, therefore, is every bit as consequential to global trade and, indeed, global stability, as a major cyber war— and even potentially more disruptive than a kinetic war. The undersea cable-scape, therefore, is undergoing a bifurcation into American and Chinese spheres of influence.

Above-water, telecoms, cloud service, data storage and other digital platform service providers have been impacted and are having to choose sides when it comes to selecting partners for new and ongoing undersea cable projects. Beyond the telecoms and tech service providers, a proxy war is playing out involving a handful of companies that engineer, manufacture, and install subsea fiber optic cables. In the context of US-China Great Power competition, this follows a general bifurcation trend affecting other strategic technologies, from semiconductors and supercomputing to advanced robotics and quantum science.



The Asia-America Gateway is the longest underwater cable, linking Southern California to landing points in Hawaii, Guam, the Philippines, China, Vietnam, Brunei, and Malaysia.

The three arenas of competition

To get foreign governments and national telecoms to reject Chinese undersea cable partners, Washington has stepped up the use of financial incentives and the application of pressure on subsea cable consortium members, including threats of sanctions and export controls.

Around the world, the geopolitics of undersea cables is playing out in three distinct arenas.

The first arena involves Washington's techno-diplomacy offensive against HMN Technologies (HMN or HMN Tech), which is majority-owned by China's Hengtong group (Hengtong).[4] The previous owner was the marine division of Huawei Technologies Co., the world's largest telecommunications equipment manufacturer and the ongoing target of US export controls and sanctions.

Since 2019, when Huawei was placed on the US Bureau of Industry and Security (BIS) Entity List, Washington has mounted a three-front war against China's national champion technology company: on the 5G infrastructure front, where US officials have attempted to persuade governments to block Huawei equipment from their networks; the semiconductor front, where critical microchip technologies have been choked off; and, finally, the subsea cables front.

As background, in early 2020, Huawei Marine Networks Co. was acquired by Hengtong Group, a Chinese state-backed optic cable manufacturer, at which time it took on its new name. Despite the name change, however, HMN has been singled out and effectively decoupled from Western-influenced undersea projects.[5]

To get foreign governments and national telecoms to reject Chinese undersea cable partners, Washington has stepped up the use of financial incentives and the application of pressure on subsea cable consortium members, including

The American tech titans are first movers not only in funding more cable gateways, but they are also pushing the innovation envelope in cable technology.

threats of sanctions and export controls. The narrative behind these actions is straightforward: If you choose HMN as a consortium partner, you choose a proxy of the Chinese Communist Party (CCP) and give Beijing eavesdropping access to all the data pulsing through your undersea cable network.

Regarding new cable deals that involve undersea linkages between American and Chinese territories, the US government has intervened and succeeded in either preventing HMN from winning any business or forcing the rerouting or abandonment of new cable deals.[6]

We will examine one of these cases, the Southeast Asia-Middle East-Western Europe 6 (SEA-ME-WE-6) cable project, along with other examples involving US allies, such as Australia and New Zealand, who have pushed out HMN's predecessor, Huawei, from underwater cable deals, at the behest of the US.
The second arena involves the emergence of tech titans as major players in the subsea cable economy. Amazon, Google, Meta, and Microsoft have been behind the rapid expansion of undersea cable networks. These firms have deep pockets and move quickly when it comes to funding new projects, but they are geopolitically agnostic when it comes to choosing partners, which sometimes puts them at odds with Washington.

The American tech titans are first movers not only in funding more cable gateways, but they are also pushing the innovation envelope in cable technology. This has placed them in a gray zone, where Washington views them as strategic partners when it comes to playing for the home team, but as security risks when they team up with the wrong consortium partners.

Beyond the geopolitical realm, Big Tech now faces increased scrutiny under antitrust laws, as they exercise control over bandwidth in their cable networks, which they increasingly rent out to telecommunications carriers and other third parties.

The third arena is perhaps the most worrisome: sabotage and outright attacks on undersea cables by adversaries. Recent events in the Baltic Sea and the Taiwan Strait involving the cutting and disabling of undersea cables reveal their vulnerabilities. These events have been linked to escalation of hostilities between Russia and the North American Treaty Organization (NATO) and the rising tensions between China and Taiwan.

We will discuss these different arenas, and how they overlap, later in this report. First, however, we examine some of the noteworthy aspects of the technology behind undersea cables.

Technology differentiators and risks

Concerns about mass surveillance and the ability to disable or shut down a cable exchange, perhaps at the command of a government, has brought heightened scrutiny to this niche industry.

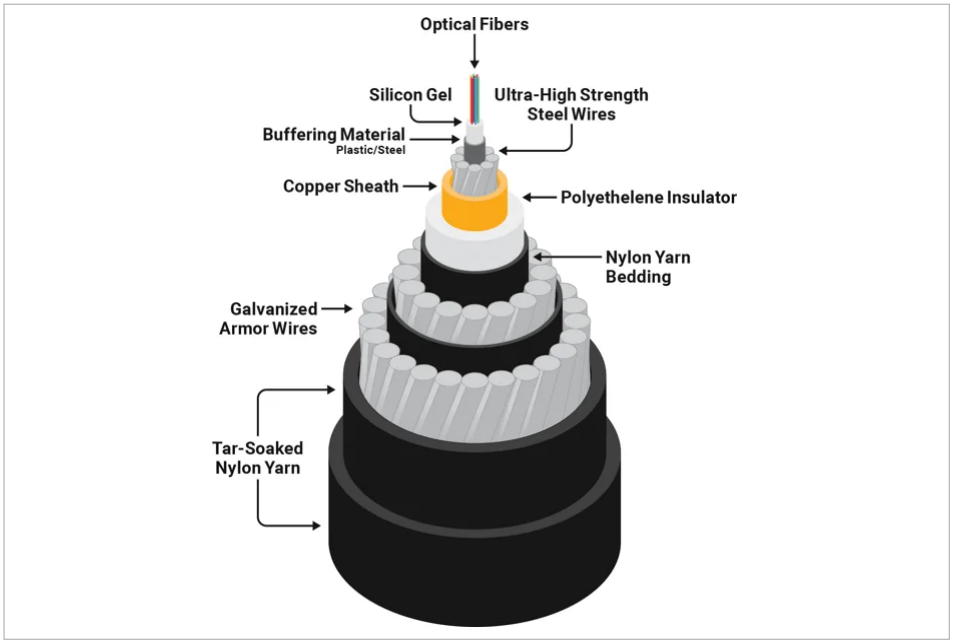
Undersea cables transmit information via pulses of light sent through optical fibers. Lasers on one end fire at rapid rates through thin glass filaments about as thick as a human hair to receptors at the other end of the cable. When bunched together inside a cable configuration, these fibers can transfer up to 250 terabits per second.

A terabit is incredibly fast and can move enormous amounts of information — imagine a super-highway with 10 trillion lanes through which data can travel simultaneously. Inside a cable, these fibers are sheathed in a few layers of insulation and protection and then wrapped in a layer of steel armor for protection — the closer a cable is to shore, the more protection it gets.

Near-shore cables are buried, but for most of the distance across the ocean floor, the average cable, which is about as thick as a garden hose, lies fully exposed.

Only about 10 nations currently have the technology to build and run these undersea cable networks: the US, a handful of its European allies, Japan, South Korea, China, and, to a lesser extent, Russia. Historically, three companies have dominated the subsea cable field: America's SubCom, NEC Corporation of Japan, and France's Alcatel Submarine Networks.

In 2008, Huawei Marine Networks became the fourth big player in the undersea cable game, and it reshaped the industry status quo. Like its parent company, Huawei Technologies, the undersea cable group benefited from generous



Components of an undersea fiber-optic cable.

government backing and funding and rapidly grew its global footprint. According to TeleGeography, a telecommunications research firm, HMN Tech grew faster than any of its competitors from 2008 to 2023 — although HMN accounted for only about 10% of global market share for subsea construction spending in 2023.[7]

Like SubCom, NEC, and Alcatel Submarine Networks, HMN designs, manufactures, deploys, maintains, and operates cable systems, which gives it exclusive physical access to its submarine technology and infrastructure, wherever it is. Here, concerns about mass surveillance and the ability to disable or shut down a cable exchange, perhaps at the command of a government, has brought heightened scrutiny to this niche industry.

Another area of concern is the landing station, where groups of cables emerge from the oceans and converge into a small gateway, in what can be described as a chokepoint. In 2023, there were about 1,400 landing stations in operation or under construction.[8] In the busiest commercial centers, landing stations take on disproportionate amounts of traffic. New York, London, and Tokyo account for much greater bandwidth than, say, Buenos Aires or Jakarta.

These landing stations have increasingly become the focal points of security-minded officials. In a US-China hybrid Cold War, decoupling over undersea cables will proceed on a scale even greater than those which have affected 5G wireless networks.

HMN designs, manufactures, deploys, maintains, and operates cable systems, which gives it exclusive physical access to its submarine technology and infrastructure, wherever it is.

Techno-diplomacy and undersea cables

The Americans are said to have created an inter-agency agency task force that has unofficially become known as 'Team Telecom,' which uses a carrot-and-stick approach to affect the outcomes of undersea cable projects.[9]

Since a paradigm shift in the West altered relations with China, the US government has taken a page out of Beijing's playbook. US diplomats at embassies around the world have pushed foreign governments and national telecommunications companies to choose SubCom, the American company, as their undersea cable partner. This would be comparable to Beijing's long-running campaign to support Huawei.

One of the things that Washington has done is deny licenses for undersea cable links that connect territories of the US with China or Hong Kong. One such project, the Pacific Light Cable Network (PLCN), announced in 2016, with substantial investments from Google and Meta, was affected. After cables had been laid from the US to the Philippines and Taiwan, approval for an offshoot of the PLCN to Hong Kong was denied by the US government — leaving hundreds of kilometers lying unused on the seafloor.[10]

On the techno-diplomacy front, in 2019, the year the US placed Huawei on the BIS Entity List, Washington began to lean harder on its allies to keep Huawei's marine division out of new cable projects in Western-aligned regions. Such was the case with the Coral Sea Cable project, when the Australian government responded to US urging by blocking Huawei Marine from participating in a cable connecting Australia with Papua New Guinea and the Solomon Islands.[11]

Earlier, in 2018, regarding the Manatua subsea cable which connects New Zealand, the Cook Islands, Niue, and Fiji, Wellington announced that it would be partnering with SubCom to develop an undersea cable network.

SPOTLIGHT

The SEA-ME-WE-6

One of the largest and most important cable projects under development is the Southeast Asia-Middle East-Western Europe 6 (SEA-ME-WE-6) undersea system. When it opens for service in 2025, the network will stretch over 19,200 kilometers, providing high-speed internet connectivity and telecommunications services to participating countries.[12] SEA-ME-WE-6 will link Singapore to Marseille in France, passing through Italy, Greece, Egypt, Saudi Arabia, Djibouti, Pakistan, India, the Maldives, Sri Lanka, Bangladesh, and Malaysia.

In 2021, the SEA-ME-WE-6 Consortium issued a request for proposals for the construction of the cable network. A number of companies submitted bids, including SubCom, and HMN Tech, the new owner of Huawei Marine.

As an enticement, and part of the Team Telecom's strategy to position SubCom as the bid winner, the US Trade and Development Agency (USTDA) reportedly gave US$3.8 million in training grants to five of the national telecom carriers along SEA-ME-WE-6's cable route, as a condition for choosing SubCom.[13] According to Reuters, Telecom Egypt and Network i2i Limited (owned by Bharti Airtel, an Indian company) each received US$1 million. Additionally, three telecom carriers representing Djibouti, Sri Lanka, and the Maldives each received US$600,000.[14]

This is textbook dollar diplomacy. The USTDA's involvement in SEA-ME-WE-6 looks just like China's approach along its Belt and Road Initiative (BRI) in say, Pakistan, where it has provided interest-free loans and open-ended credit to telecoms carriers for their purchase of Huawei or ZTE equipment.

The SEA-ME-WE-6 undersea system will stretch over 19,200 kilometers, providing high-speed internet connectivity and telecommunications services to participating countries.

US diplomats say that under China's Military-Civil Fusion (MCF) system — the requirement that all strategic technologies must flow into the People's Liberation Army (PLA) purview — HMN Tech would pass restricted technology on to the PLA and, thus, would end up on a US sanctions list.

For a government or telecom company, the possibility of sanctions made the selection of HMN Tech a virtual non-starter. If the US were to enforce restrictions on HMN Tech, any money invested in the Chinese subsea company would likely become a loss-making venture.

US diplomats wrote letters or held meetings with telecoms executives, in, among other places, Bangladesh, Singapore, and Sri Lanka. US officials stressed the threat of sanctions and pointed out the benefits of a security partnership with the US. Regarding national security, US officials also drew attention to the possibility of espionage through Chinese-made undersea technologies.

At decision time, the SEA-ME-WE-6 Consortium awarded the contract to SubCom, even though its bid was reportedly higher than HMN Tech's. Despite having a higher bid than HMN, the consortium decided to go with SubCom largely because of the threat of crippling US sanctions on the Chinese company.

SubCom is a well-established undersea cable company known for the high quality of its expertise in cable design, manufacturing, and installation. But now that Washington has made the company its national champion, it seems clear that in today's geopolitical landscape, it will no longer be competing solely on price.

After the SEA-ME-WE-6 outcome, HMN Tech, China Mobile and other partners went on to build a direct competitor, the PEACE cable, which connects Asia, Africa, and Europe.[15]

Despite having a higher bid than HMN, the consortium decided to go with SubCom largely because of the threat of crippling US sanctions on the Chinese company.

The state versus firms in the gray zone

Going forward, the likelihood of an undersea cable project being completed is much higher when its major investors are Big Tech companies, rather than when governments have majority control.

Since 2019, demand for internet bandwidth has tripled.[16] The migration of more and more data to the cloud and the increase in connected devices has fuelled a data renaissance. When it comes to the funding, building, and ownership of bandwidth, the world has witnessed another kind of paradigm shift, this one regarding the role of traditional telecoms and Big Tech.

Amazon, Google, Meta, and Microsoft now exert more control over data flows in subsea cables than traditional telecoms carriers. In fact, the roles of the two have almost reversed - Traditional voice carriers now rent increasing swathes of their bandwidth from the tech titans. Dedicated cables owned by Google or Microsoft allow them more control over their growing data centers with their customized data platforms.

As for money, Big Tech has a lot of it. In 2023, Google, alone, owned 26 undersea cables.[17] This trend is set to continue as Meta, Amazon, and Microsoft, all of which own or partially own their own cables, set out to expand their own dedicated networks. Going forward, the likelihood of an undersea cable project being completed is much higher when its major investors are Big Tech companies, rather than when governments have majority control.

With all of this, there is a duality involved in the relationships between states and firms regarding undersea cables. More specifically, the American tech giants are viewed as strategic assets and partners, when it is in Washington's best interests to treat them as such. But, conversely, when Meta or Google undertake business dealings with perceived adversaries, the consequences can involve aborted cable routes and sanctioned partners.

Dedicated cables owned by Google or Microsoft allow them more control over their growing data centers with their customized data platforms.

Statecraft, sabotage, and war

In early 2023, two undersea communications cables running from Taiwan to the nearby Matsu islands were mysteriously cut, disconnecting 14,000 islanders from the internet. Taiwanese officials blamed the incident on a Chinese fishing vessel and freighter which had been spotted in the area.[18]

Later that year, Finland and Estonia began a formal investigation of a Chinese vessel that dragged its anchor over 100 nautical miles across the seafloor though the Gulf of Finland, damaging undersea cables and gas lines.[19]

The Chinese-owned container ship, The New Polar Bear, was seen together with a Russian cargo vessel, the Sevmorput, passing through the Gulf of Finland and were alleged to have been in close proximity to where damage to an undersea natural gas pipeline and two telecommunications cables occurred.[20]

Such incidents are harbingers of more to come, especially with the threat of escalating conflicts. NATO officials have claimed that Russia has been actively mapping critical allied infrastructure, both undersea and on land.[21] This may be an indication of Moscow's future intentions, should the war in Ukraine escalate.

As far back as the 1980s, the US intelligence community engineered a stunning wiretapping operation on Soviet communication cables beneath the Sea of Okhotsk, in an operation code-named Ivy Bells.[22]

To carry out the operation, the US Navy equipped a specially designed submarine, the USS Halibut, with specialized devices that allowed it to tap into undersea cables without damaging them. A specialized arm with a grappling hook was used to snag the cable and bring it close to the submarine; a robotic cutting device cut a small section of the cable sheath, and a tapping device was connected to the exposed cable which intercepted the signals transmitted through the cable.

The signals were sent to the US National Security Agency (NSA) for analysis, providing valuable intelligence about Soviet military and diplomatic plans. The operation ran from 1972 to 1981 when the Soviets finally discovered it and shut it down.

Technology has evolved significantly since the days of Operation Ivy Bells. Today's submarines are equipped with even more sophisticated devices, including fiber-optic tapping devices that can tap into cables without cutting them. Other advanced technologies include software-defined radios that can be programmed to intercept a wide range of frequencies, including those used for undersea communications.

The story of undersea cable espionage and sabotage is in its early stages, but one thing is for sure - the technologies used to carry out the next generation of electronic undersea espionage will evolve.

All this will have a major impact on how billions of people receive data, voice, picture, and streaming video on the internet, whether or not they are aware of the struggle over undersea cables that deliver these media.

Researcher bio: Alex Capri

Alex Capri

Research Fellow, Hinrich Foundation; Senior Lecturer, National University of Singapore

Alex Capri is a research fellow at the Hinrich Foundation and a lecturer in the Business School and Lee Kuan Yew School of Public Policy at the National University of Singapore.

He is the author of *Techno-Nationalism: How it's reshaping trade, geopolitics, and society* (Wiley), due out in May 2024.

From 2007-2012, Alex was the Partner and Regional Leader of KPMG's International Trade & Customs Practice in Asia Pacific, based in Hong Kong. Alex has over 20 years of experience in global value chains, business and international trade – both as an academic and a professional consultant.

He advises governments and businesses on matters involving trade and global value chains. Areas of focus include: IT solutions for traceable supply chains, sanctions, export controls, FTAs and trade optimization.

Alex has been a panelist and workshop leader for the World Economic Forum. He writes a column for Forbes Asia, Nikkei Asia and other publications and is a frequent guest on global television and radio networks.

He holds a MSc from the London School of Economics in International Political Economy and a BSc in International Relations from the University of Southern California.

***

Other Hinrich Foundation publications by Alex Capri:

- How enforceable are "progressive" standards in multilateral FTAs?
- Strategic US-China decoupling in the tech sector
- Semiconductors at the heart of the US-China tech war
- Techno-nationalism and the US-China tech innovation race
- Techno-nationalism and diplomacy
- India: A 21st century technology hub?
- Quantum computing: A new frontier in techno-nationalism
- The geopolitics of climate change and cleantech
- After Ukraine: The new geopolitics of food security
- Geopolitics and the race for data supremacy
- How Starlink and satellite internet are reshaping geopolitics in space
- AI arms race shakes tech, trade, and truth
- The in-China-for-China corporate gray zone

And more on **hinrichfoundation.com**

Endnotes

1. The Economist. (2023, December 20). Big tech and geopolitics are reshaping the internet's plumbing. https://www.economist.com/business/2023/12/20/big-tech-and-geopolitics-are-reshaping-the-internets-plumbing
2. TeleGeography. (n.d.). Submarine cable: Frequently asked questions. https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
3. Siebold, S. (2023, May 3). NATO says Moscow may sabotage undersea cables as part of war on Ukraine. Reuters. https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/
4. Hengtong Group. (n.d.). Submarine system. http://www.hengtonggroup.com/en/home/products/index/categoryId/3.html
5. HMN Technologies Co. Ltd. (2020, November 3). Huawei Marine Networks rebrands as HMN Technologies [Press release]. HMNTech. https://www.hmntech.com/enPressReleases/37764.jhtml#:~:text=In%20the%20first%20half%20of,New%20Saxon%202019%20Ltd.
6. Brock, J. (2023, March 24). U.S. and China wage war beneath the waves – over internet cables. Reuters. https://www.reuters.com/investigates/special-report/us-china-tech-cables/
7. The Economist. (2023, December 20). Big tech and geopolitics are reshaping the internet's plumbing. https://www.economist.com/business/2023/12/20/big-tech-and-geopolitics-are-reshaping-the-internets-plumbing
8. TeleGeography. (2023). Submarine cable map 2023. https://submarine-cable-map-2023.telegeography.com/
9. Brock, J. (2023, March 24). U.S. and China wage war beneath the waves – over internet cables. Reuters. https://www.reuters.com/investigates/special-report/us-china-tech-cables/
10. Office of Public Affairs. (2020, June 17). Team Telecom recommends that the FCC deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States [Press release]. U.S. Department of Justice. https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea#:~:text=Team%20Telecom%20today%20recommended%20to,United%20States%20and%20Hong%20Kong.
11. Packham, C. (2019, August 28). Ousting Huawei, Australia finishes laying undersea internet cable for Pacific allies. Reuters. https://www.reuters.com/article/idUSKCN1VI08H/
12. SEA-ME-WE 6. (2024, February 24). In Wikipedia. https://en.wikipedia.org/wiki/SEA-ME-WE_6#:~:text=Bangladesh%2C%20Singapore%2C%20Malaysia%2C%20Indonesia,ME%2DWE%2D6%20Consortium.
13. Brock, J. (2023, March 24). U.S. and China wage war beneath the waves – over internet cables. Reuters. https://www.reuters.com/investigates/special-report/us-china-tech-cables/
14. Ibid.
15. Clark, R. (2020, January 24). Hengtong set to shape the global subsea market. Submarine Telecoms Forum. https://subtelforum.com/hengtong-set-to-shape-the-global-subsea-market/
16. The Economist. (2023, December 20). Big tech and geopolitics are reshaping the internet's plumbing. https://www.economist.com/business/2023/12/20/big-tech-and-geopolitics-are-reshaping-the-internets-plumbing

17. Ibid.
18. Wu, H., & Lai, J. (2023, April 18). Taiwan suspects Chinese ships cut islands' internet cables. Associated Press. https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70
19. Tegler, E. (2023, November 28). Investigating the Chinese ship that 'accidentally' hit undersea lines. Forbes. https://www.forbes.com/sites/erictegler/2023/11/28/investigating-the-chinese-ship-that-accidentally-hit-undersea-lines/?sh=55e4238f40bf
20. Ibid.
21. Siebold, S. (2023, May 3). NATO says Moscow may sabotage undersea cables as part of war on Ukraine. Reuters. https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/
22. Operation Ivy Bells. (2024, February 24). In Wikipedia. https://en.wikipedia.org/wiki/Operation_Ivy_Bells

hinrich foundation

advancing sustainable global trade

The Hinrich Foundation is an Asia based philanthropic organization that works to advance mutually beneficial and sustainable global trade.

We believe sustainable global trade strengthens relationships between nations and improves people's lives.

We support original research and education programs that build understanding and leadership in global trade. Our approach is independent, fact-based, and objective.

CONTACT US

There are many ways you can help advance sustainable global trade. Join our training programs, participate in our events, or partner with us in our programs.

inquiry@hinrichfoundation.com

Receive our latest articles and updates about our programs by subscribing to our newsletter

hinrichfoundation.com

hinrichfdn
hinrich foundation
hinrichfoundation
hinrichfoundation