

Note: Below is an article published by The Financial Times (13th June 2023) and as referenced below.

How the US is pushing China out of the internet's plumbing

Nearly 1.4mn kilometres of metal-encased fibre criss-crosses the world's oceans, speeding internet traffic seamlessly around the globe. The supply and installation of these cables have been dominated by companies from France, the US and Japan.

The Chinese government started successfully penetrating the global market, but consecutive US administrations have since managed to freeze China out of large swaths of it. This was ostensibly because of concerns of espionage and worries about what Beijing might do to disrupt strategic assets operated by Chinese companies in the event of a conflict.

Despite being routinely blocked from international subsea cable projects involving US investment, Chinese companies have adapted by building international cables for China and many of its allied nations.

This has raised fears of a dangerous division in who owns and manages the infrastructure underpinning the global web.

Blocking Beijing

This online Financial Times article by Gross (2023) assesses the ongoing US national security concerns posed by China's original involvement in major subsea cable infrastructure:

In 2018, Amazon, Meta and China Mobile agreed to work together on a cable connecting California to Singapore, Malaysia and Hong Kong. But a spate of manoeuvres in Washington to block Chinese participation in US cables led to China Mobile pulling out of the consortium. Meta and Amazon filed a new application for the system in 2021, this time with no Chinese investment, no connection to Hong Kong, and a new name: Cap-1. Then, last year, the application for Cap-1 was withdrawn altogether, even though most of the 12,000km cable had already been built. China's original involvement remained a security concern for the US government, according to two people briefed on the discussions. "There are hundreds of millions of dollars sunk in the Pacific," said a person involved in the aborted project. Meta and China Mobile did not respond to requests for comment. Amazon declined to comment. Over the last five years, as tensions between the two countries have mounted and fears have grown in Washington about the risks of espionage, the US government has sought to pull apart an interwoven network of internet cables that had developed through international collaboration over decades.

Gross(2023)

Gross(2023) outlines further in the Financial Times how it appears the US is waging a fibreoptic war against China, restricting its (China's) involvement in major submarine cable laying projects now and in the future:

The US has succeeded in preventing Beijing from becoming a major player in the global submarine cable market. Chinese supplier HMN Tech has provided or is set to provide the equipment to only 10 per cent of all existing and planned global cables, where the supplier is known, FT analysis of data supplied by the consultancy TeleGeography shows. Meanwhile, French cable maker ASN has supplied 41 per cent and American company SubCom has supplied 21 per cent. Neither ASN nor SubCom responded to requests for comment. And interviews with more than 20 industry executives suggest Washington's campaign has resulted in a de facto ban on using a Chinese supplier across swathes of the industry, even in projects where there is no US involvement. Some are worried this could fracture the global internet as Chinese companies start building their own cable networks elsewhere.

"One of the big risks right now is heading in the direction of bifurcated networks. Does this create a system where you don't have connectivity, with a quasi-cold war, eastern bloc versus the west?" says April Herlevi, an expert in China's foreign economic policy at the Center for Naval Analyses. "I don't think we're there yet . . . but I do worry that's the direction we're headed in."

Several countries, including China, Pakistan, Saudi Arabia and Russia, have been overt about their ambitions to create a more centralised internet infrastructure over which their governments would have greater control. They have also shown themselves willing and able to turn off access to certain sites, or even the whole internet, during times of political turbulence. But US efforts to exclude Chinese companies from the world's internet backbone are mired in difficulties. Even as the US administration wages its fiberoptic war against Beijing, vessels owned and manned by China are still undertaking complex repair work on US-owned fibre lines, people with direct knowledge of such operations have told the Financial Times. Meanwhile, new analysis shows more data is flowing between the US and China than at any other point in history, even if the route between the two is often less direct than before. Several people in the industry point out that data can still be intercepted even if the infrastructure carrying it is not built by Chinese companies.

Gross(2023)

A Cold War Under The Sea

Gross (2023) now delves into the intricacies of the deep sea cable network and its geopolitical repercussions in this Financial Times article piece.

There are more than 500 active and planned submarine cables, transporting 99 per cent of intercontinental data, arriving at around 1,400 coastal landing stations around the world. TeleGeography, a consultancy for the sector, estimates that more than \$10tn-worth of financial transactions are transmitted via these cables every day.

For the most part, consortiums of tech and telecoms companies build the cables, and often resell bandwidth on the fibre lines to customers around the world. An email sent from London to New York across one of these cables can travel in under 70 milliseconds (0.07 seconds). Satellites, by contrast, are able to carry far less data and are much more expensive to launch and run. They account for a tiny fraction of intercontinental data transport and will do so for decades to come. For years, the subsea cable sector was driven by investments from largely state-owned telecoms operators, but over the past decade tech groups have taken their place. US tech behemoths, including Google, Meta and Microsoft, invested about \$2bn in cables between 2016 and 2022, accounting for 15 per cent of the worldwide total. Over the next three years, they will pump in a further \$3.9bn, or 35 per cent of the total. They did not respond to requests for comment. These tech groups are also big consumers of cable capacity. According to TeleGeography, they account for two-thirds of bandwidth usage.

While over the past decade the sector was being reshaped by greater investment from US tech companies, a parallel story was emerging. In 2015, the Chinese government announced a strategic initiative to invest huge amounts in developing countries' communications, surveillance and e-commerce capabilities in exchange for diplomatic influence. Internet cables were key to this "Digital Silk Road", which ran in parallel to Beijing's Belt and Road Initiative that has pumped hundreds of billions into building roads, railways and ports across the developing world. The Chinese telecoms champion Huawei was at the time successfully carving a niche in the submarine cable market, via its joint-venture Huawei Marine, which it owned almost equally with the UK-based submarine cable installer Global Marine.

Fuelled by Beijing's ambition, Huawei Marine managed to capture about 15 per cent of the global market by 2019, according to Mike Constable, who was chief strategy officer of China's largest cable supplier until March this year and chief executive at the time it was co-owned by Huawei. But this was "before the geopolitics went crazy", he says.

In 2019, the Trump administration imposed sanctions on Huawei and the telecoms group swiftly divested from the submarine cable joint venture. A little known regional Chinese cable manufacturer, Hengtong Group, bought Huawei Marine and renamed it HMN Tech. Today, only one HMN Tech-supplied cable is due to come online in each of the years 2024 and 2025, each connecting China exclusively to south-east Asian countries.

In 2020, the US government also created the Clean Network initiative, in effect banning new cables directly connecting the US to China or Hong Kong. A landmark cable being built by Meta and Google that was set to connect the US with Hong Kong was blocked by Washington when construction was already underway. The Pacific Light Cable Network, which went live last year, now terminates in the Philippines and Taiwan. Meanwhile, for HMN Tech, "the bid [invitations] coming through the door started to dry up", Constable says.

In 2021, following pressure from the US government, the World Bank scrapped a cable project it was leading to connect three Pacific island nations, to avoid awarding the contract to HMN Tech. And last year a successful two-year campaign by US officials, first reported by Reuters, culminated in the consortium planning the 19,000km Sea-Me-We 6 cable from south-east Asia to Europe awarding the contract to US supplier SubCom after initially selecting HMN Tech. The consortium behind two linked upcoming cables, one of which will connect Europe to Jordan and the other Jordan to India, did not invite HMN Tech to bid at all, according to a source close to the projects, because Google is a key investor. HMN Tech did not respond to requests for comment. But projects with US investors or direct links to the country are not the only ones affected by the Clean Networks initiative and sanctions that the US government imposed on HMN Tech in 2021. As the tendrils of Washington's foreign policy

gradually weave across the globe, several consortiums building cables that neither connect to the US nor have US financing are now excluding HMN Tech, multiple interviews suggest.

“When you build a cable you have to look at which customers you’re going to target. If you want to work with hyperscalers like Google, Meta, Microsoft, you have to think about if you want Chinese equipment,” says Chris Van Zinnicq Bergmann, chief commercial officer of the upcoming Mediterranean cable Unitirreno. Invariably, he added, “the answer is no”.

A new cable project connecting Singapore and Thailand to India, which has no American owners and will not touch US territory, is not expected to invite HMN Tech to bid because of the geopolitical situation, says a person with knowledge of the project. Another person said they were currently involved in two separate upcoming cables “where for political and funding reasons” the investors “decided not to engage Chinese companies in the tendering process” even though there is currently no connection to the US or US investment. Increasing hostility between China and the west is already pushing companies to forge new routes along which to send data traffic. Disputes over territorial waters, delays to permits and the US government’s ban on cables directly connecting China or Hong Kong to the US have contributed to multiple recent cable consortiums - Apricot, Bifrost and Echo - forging a new path through Singapore, Indonesia, the Philippines and the US island territory of Guam, which is emerging as an unlikely hub for international data traffic.

A spokesperson for the US state department says: “The continued health of the global internet depends on the free flow of data across borders, facilitated by trustworthy telecommunications infrastructure.”

“Countries should prioritise national security, data security and privacy by putting in place appropriate policy and regulatory frameworks that fully exclude untrustworthy vendors from the entire ICT ecosystem, including wireless networks, terrestrial and undersea cables, satellites, cloud services and data centres,” the spokesperson adds.

Gross(2023)

China’s Shifting Focus And Ambitions

Gross (2023) here discusses how China has managed to gain ground in the deep sea cable race.

Though China’s ambition to become a major contender in the global market for subsea cables has been thwarted, Beijing is still finding ways to gain ground. Industry insiders say Chinese government-owned telecoms companies have tried to shift their focus to regions where they do still have commercial and political influence.

“China is able to lead projects in some Asian, African and Latin American countries, mainly because state-owned telecom companies can fight price wars well,” a person working for the Chinese government said.

In Asia, where demand for bandwidth and the cables that carry it is growing faster than many other regions in the world, China Telecom, China Mobile and China Unicom are currently leading several big cable projects, including two that will connect China to Singapore and Japan. The three companies did

not respond to requests for comment. China's infrastructure empire-building around Africa and Europe was successful for many years. China Unicom was a key investor in Sail, a 5,800km cable connecting Brazil with Cameroon that went live in 2020. China Mobile was also crucial to a flagship cable consortium, 2Africa, connecting large swathes of Africa with Europe on which work started in 2020. It counts Meta and Vodafone as investors.

It is, however, unlikely that Chinese companies would enjoy the same freedom to build a cable with western groups and connect it to European ports today. The provisions of the Clean Networks Initiative "are becoming more onerous very quickly", according to a lawyer working in the industry. "They're getting stricter as we speak."

But Peace, a cable that went live last year connecting Pakistan to France via Kenya, was entirely financed and built by Chinese companies, including HMN Tech, thereby circumventing the need for the groups to be invited to the table by western companies. France's president, Emmanuel Macron, has signalled his interest in maintaining economic and trade interests with China. "Peace is really part of the new Silk Road, from China to Europe," said an executive at a big European telecoms company, noting that it is one of the early examples of China opting to finance and build a project without any input from international companies. Several industry executives told the FT that while HMN Tech is still seen as trailing behind its global competitors in terms of the quality of its technology, it routinely submits bids to work on international projects priced 20 to 30 per cent below what competitors would charge. Savvy investors have caught on, inviting HMN Tech to bid for projects solely to push the price down, they say.

"They are used as a stalking horse on pricing because they are known to [be] very, very aggressive," said an executive at a rival cable group. HMN Tech was invited to bid on the Medusa cable, connecting Egypt to Portugal, and Africa-1, connecting Kenya to France, but was ultimately passed over for French operator ASN, according to industry sources. China has other levers it can pull to fight back against international curbs. As well as becoming more protective of its offshore territory generally, it has started applying a lot of pressure on companies laying cables through Chinese waters and the South China Sea to use cable produced by HMN Tech, according to two industry executives working on projects in the region. Chinese companies have also commissioned three vessels to lay and maintain cables, to reduce the nation's dependence on foreign ships, according to Constable. "China now sees the ability to build its own cables as strategically important, because no one else can do it for them," he says.

"The South China Sea is one of the most critical sea areas in China's military strategy. Every link and component of the infrastructure must be controllable," the person working for the Chinese government said.

Gross(2023)

The Espionage Threat

Gross(2023) here assesses the ongoing threat of industrial espionage and US national security concerns, posed by China's original involvement in major subsea cable infrastructure:

Growing anxiety about the vulnerability of cables to espionage and sabotage has led some governments to become more protective of their territorial waters, causing delays to the receipt of permits for both laying and maintaining cables. Several countries, including Indonesia and Canada, have begun mandating that only certain ships and personnel can lay and maintain cables within their exclusive economic zones, industry executives say.

And because of complex, long-standing maintenance agreements, often countries' most sensitive, critical infrastructure is being repaired by adversarial nations. A fault last year on a major intercontinental fibre cable owned by US carriers AT&T and Verizon, among others, was repaired by Chinese engineers operating from a Chinese vessel. In the same year, the same ship fixed another faulty cable in the East China Sea, part-owned by Microsoft and Japanese telecoms group SoftBank, according to people briefed on the activities. AT&T, Verizon, Microsoft and SoftBank did not respond to requests for comment. Industry insiders point out that the moments at which this maintenance work is carried out are some of the greatest points of vulnerability to hacking and damage in a cable's lifespan — given devices could be inserted to capture or corrupt data.

“When governments think about subsea cables' exposure to faults and malicious disruption, I don't think they understand how the maintenance market works,” says Constable. The US “has been trying to bifurcate this global network of subsea cables but didn't look at whose cable ships were repairing whose cables”.

While tapping cables at sea is widely agreed to be very difficult, some say it is possible to insert data extraction devices into repeaters — the electronic components that connect different sections of cables to keep the signal moving over longer distances — when manufacturing or repairing the cables. UK intelligence service GCHQ has previously collected bulk data from international cable landing stations on the British coast, the Snowden leaks revealed, while in 2020 a whistleblower accused the US National Security Agency of teaming up with Danish government agencies to spy inside landing stations.

Some argue that who owns subsea cables and landing stations is something of a moot point, as data travels across borders in a relatively unregulated way and can still be accessed when passing through a nation's territory even if the route is less direct. Alan Mauldin, research director at TeleGeography, points out that the rapid transmission and decentralised nature of the internet means that Washington's tightening restrictions “do nothing to stop the flow of data between China and the US”. James Lewis, director of technology and public policy at the Center for Strategic and International Studies in Washington, argues that fears around fragmentation are overstated. Beijing's main interest, he argues, is not a separated network, but instead greater access to information and trade. “They want business,” he says. “The Chinese don't want to break the internet, they want to own it.

Gross(2023)

References

Gross, A., Heal, A. C., Clark, D., Bott, I., & de la Torre Arenas, I. (2023, June 13). *How the US is pushing China out of the internet's plumbing*. Retrieved from Financial Times: <https://ig.ft.com/subsea-cables/>