CSS | ISSUE BRIEF

The Tension Under the Sea: Analyzing International Security Concerns Related to Undersea Cable Networks

Sahej Veer Singh*

Edited by: Mihir Vikrant Kaulgud

Introduction

On July 29, 1858, two steam-powered battleships met in the middle of the South Atlantic ocean, linking the ends of a 4,000-kilometre-long cable that telegraphed the North America and Europe for the first time. A procession through the New York streets was followed by a congratulatory telegram from Queen Victoria to then-US President James Buchanan. While Queen Victoria praised the two countries for their great international endeavour (the conclusion of over two decades of struggle), Buchanan called it a "triumph more magnificent than was ever achieved by conqueror on the battlefield." The message had taken nearly 17 hours to travel, with each letter taking 2 minutes and 5 seconds in Morse code. Owing to several technical problems, the inaugural cable lasted just about a month before turning dysfunctional. Nevertheless, everyone knew that a worldwide information revolution had begun.[1]

Submarine cables for telecommunications were an early catalyst for globalization and multinational market structures, and they continue to support massive global economic activity. The first undersea telephone cable, Transatlantic No. 1, was built in 1956. By 1988, TAT-8 carried 280 gigabytes per second through fibre optic cables, which used light to transmit information at breakneck speeds. The *Marea* cable was launched in 2018, linking Bilbao, Spain, and Virginia, the United States, with transfer rates of up to 160 tbps (Sixteen million times higher than the typical household internet connection). Today, there are roughly

* ***The Author is a student at the Jindal School of International Affairs and Research Assistant at the Centre for Security Studies, JSIA.***

[1]Griffiths, James. "The Global Internet Is Powered by Vast Undersea Cables. but They're Vulnerable." *CNN. Cable News Network*, July 26, 2019. https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html.

380 undersea cables in use worldwide, with a total length of more than 1.2 million kilometres (or 745,645 miles). With many of them being financed by internet giants like Facebook, Google, Microsoft and Amazon, underwater cables are the unseen power that drives the contemporary Internet. According to Byron Clatterbuck, the CEO of Seacom, "most people are very shocked" by how much of the Internet is still cable-based.[2]

Historical Context

At the initial stages, private investment played a critical role in the internet revolution. In 1892, 89.6 per cent of the 246,871 km of cables in situ was private, with just 10.4 per cent being government-owned. Although these lines extended to every continent, the technology and expertise remained firmly in the hands of limited British elite. The 257 private cables controlled by British corporations accounted for 63.1 per cent of the world total. Lines that connected areas where commercial clients were prevalent, like between London and New York, benefited significantly from these technological developments. Eventually, governments got engaged in this trend as well. However, the Chinese government did not embrace telegraph technology and repeatedly rejected permission to connect Shanghai until 1875, which is when a state-owned network was seen as vital for governance. On the contrary, countries like Africa were connected for political reasons only, for example, to efficiently connect coastal colonial settlements.[3]

Today, tech giants like Microsoft, Facebook, and Google are increasingly involving themselves in the cables business. Facebook has built a cable from scratch for the first time rather than financing existing programs or borrowing wires. Similarly, the Hawaiki Submarine Line was purchased by Amazon Web Services (AWS) last year to boost efficiency for its cloud clients. Content providers currently account for 38% of all international bandwidth usage worldwide. According to Jon Hjembo, an analyst at

[2] Malecki, E., and Hu Wei. “A Wired World: The Evolving Geography of Submarine Cables and the Shift to Asia: Semantic Scholar.” undefined, January 1, 1970. https://www.semanticscholar.org/paper/A-Wired-World%3A-The-Evolving-Geography-of-Submarine-Malecki-Wei/2cd54571e1a4eeee3869b9031c678b553bb86f6d.

[3] “Bench Talk.” Submarine Cables: Long-Distance Pathway for Internet Data | Bench. Accessed December 11, 2021. https://www.mouser.in/blog/submarine-cables-long-distance-pathway-for-internet-data.

TeleGeography, “[t]here are a handful of very, very influential content providers who are shifting the balance away from the telecoms.”[4]

However, international telecommunication is "not merely a business but also a political venture, it is the subject of great-power rivalry". The first trans-Pacific cable was built in response to the US Navy's discovery that transmissions between Washington and the Philippines were routed via British cables to Hong Kong and Manila.[5]

International Security Concerns

With the dynamic development of undersea cables come various concerns for the international community. In 2012, Hurricane Sandy smashed into the US East Coast, causing $71 billion in damages and ruining many critical underwater cable exchanges connecting North America and Europe. [6] Frank Rey, director of worldwide network planning for Microsoft's Cloud Infrastructure and Operations business stated in an interview, “[i]t was a huge disturbance. For several hours, the whole network between North America and Europe was down. The hurricane exposed a possible difficulty in the consolidation of transatlantic cables that all terminated in New York and New Jersey for us.”

As a result, Microsoft opted to site its US operation for *Marea* (its newest cable) further down the coast in Virginia to remove any interruptions in case another massive storm disrupted New York. Each year, around 200 failures occur, most of which are initiated by people. According to Tim Stronge, vice-president of research at TeleGeography, “two-thirds of cable failures are caused by inadvertent human activity such as fishing nets and trawling, as well as ship anchors.”[7] Similar to the Hurricane Sandy incident, in 2006, a 7.0 magnitude

[4] Ball, James. “Facebook and Google's New Plan? Own the Internet.” WIRED UK, October 7, 2021. https://www.wired.co.uk/article/facebook-google-subsea-cables.

[5] “Submarine Telegraph Cables: Business and ... - Jstor Home.” Accessed December 11, 2021. https://www.jstor.org/stable/3116386.

[6] Darrow, Barb. “Superstorm Sandy Wreaks Havoc on Internet Infrastructure.” Gigaom. Gigaom, June 9, 2020. https://gigaom.com/2012/10/30/superstorm-sandy-wreaks-havoc-on-internet-infrastructure/.

[7] Griffiths, James. “The Global Internet Is Powered by Vast Undersea Cables. but They're Vulnerable.” CNN. Cable News Network, July 26, 2019. https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html.

earthquake off the southwest coast of Taiwan severed eight underwater cables, causing internet blackouts and massive chaos in Japan, Hong Kong, Taiwan, China, Philippines and Korea.[8] Similarly in February 2008, a large region of the Persian Gulf and North Africa fell out, owing to the damage caused to 3 underwater cables off the coast of Egypt. According to the cable's owner, at least one cable (connecting Oman and Dubai) was destroyed by a 5,400-kilogramme anchor. A major concern to underwater cables is purposeful human attacks. British politician Rishi Sunak argued in a 2017 study that "security remains an issue" for underwater cables. "The arteries upon which the Internet and our modern world rely have been left highly vulnerable," he said. "Funneled through exposed choke points (often with minimal protection) and their isolated deep-sea locations entirely public, the arteries upon which the Internet and our modern world rely have been left highly vulnerable." He added that, "the risk of these flaws being exploited is increasing. The security and prosperity of the United Kingdom would be severely harmed if the attack was successful."[9]

Although it is theoretically conceivable to tap the modern-day fiber optic cables, it is far easier to cut or destroy them, causing substantial disruption to consumers. While specific placement of undersea cables is unknown, advances in "bottom survey" technology are making it simpler to locate them. The interruption in communications for a few minutes or seconds can be disastrous in time-sensitive army missions, and even milliseconds can cost millions in financial transactions. Although most of the cable failures do not cause complete stoppage, they can reduce data transmission speeds significantly. Most cable breakages occur in very shallow water due to harsh weather causing the wires to snap, or even fishing trawlers catching cables in nets. Some outages, on the other hand, have more sinister sources. Aside from the undersea cables themselves, on-ground termination locations are more dangerous and even simpler to locate. These places are frequently the intersection of many cables. A strike on one of them might have the same impact as severing numerous cables at once.

[8] Qiu, Winston. "Winston Qiu." Submarine Networks, March 19, 2011. https://www.submarinenetworks.com/news/cables-cut-after-taiwan-earthquake-2006.

[9] Sunak, Rishi. "Undersea Cables: Indispensable, Insecure." Policy Exchange, June 5, 2018. https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/.

Spying

Tapping undersea networks isn't a new activity. During the Cold War, US submarines sent professional divers to the Sea of Okhotsk with specially designed equipment to track and disrupt Soviet communications. The covert monitoring lasted around 10 years until Ronald Pelton; an NSA communications specialist leaked information about the activity.[10] More than 99 per cent of global communication is now transmitted by fiber optic cables, the majority of which is through undersea cables. Surveilling contemporary fiber optic cables is considerably more difficult, but not impossible, than tapping underwater phone lines. According to AT&T Labs researchers, attackers might disable parts of a system that they can't monitor and redirect users to channels that they already control, without the victim realising that their communications are being broadcast.

As mentioned before, the simplest method to do so is to tap the place where the cable links to the land rather than the cable itself. This is what the UK and US surveillance services have already been accused of doing with help of the big businesses which operate the cable networks. The Guardian in 2013 claimed that GCHQ (British spy agency) has "secretly obtained access to the network of cables that transport the world's phone conversations and internet traffic," using papers provided by famous NSA whistleblower Edward Snowden. If documents given by Snowden are observed, GCHQ was processing 600 million so called "communications events" per day and hacked more than 200 fiber-optic lines. According to a presentation provided by Snowden, the NSA launched a similar operation named Upstream, which was able to intercept "communications on optic fiber and equipment as data flows through." GCHQ declined to give comments to the Guardian. An NSA spokeswoman claimed the organization "neither can confirm nor deny mission-related actions."[11] Her statement also said that "privacy and civil rights are fundamental priorities in the NSA's mission design and implementation."

[10] Company, Sudo Null. "Sudo Null - Latest It News." SudoNull. Accessed December 11, 2021. https://sudonull.com/post/52678-Messages-in-depth-the-amazing-story-of-the-underwater-Internet-ua-hostingcompanys-blog.

[11] "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications." The Guardian. Guardian News and Media, June 21, 2013. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

The USS Jimmy Carter submarine has extensive undersea network tapping capabilities inside it that makes the job of tapping wires simple. America is not the only country suspected of engaging in such behaviour. According to US intelligence sources, underwater sensors saw Russian military submarines near major communication cables in 2015, in addition to a spy ship carrying mobile underwater devices meant destroy network lines. The authors of a 2016 study by the Center for Strategic and International Studies wrote:

> "It is probable that Russian auxiliary vessels, such as tele-operated or independent undersea craft, have been fitted to really be capable of manipulating objects on the ocean bottom and could also convey sensitive communications obstruct devices in order to tap submarine cables or otherwise destroy or exploit seafloor infrastructure." [12]

The US-China Rivalry

In June 2020, Washington voiced opposition to a new proposal from Facebook and Google to construct an underwater internet network between Honk Kong and US. The Justice Department concluded that it is too hazardous and provides "unprecedented chances" for Chinese government spying. On June 17, Team Telecom (which has recently been in the headlines for inadequate inspections) suggested that the Federal Communications Commission suspend the connection to Hong Kong.[13] Hacking the opponent's intelligence system is just one way to project geopolitical power on the Internet; constructing and maintaining underwater cables, landing stations and all the other practical network is critically important in the digital battle and is now a major security concern. Undersea cables are only one part of a much more problematic and strategic geopolitical battle.

In 2016, Facebook and Google became partners in the Pacific Light Cable Network project. The US giants collaborated with TE SubCom and Pacific Light Data Communication Company to be onboard a project that had been in the works for months: building a massive undersea internet cable connecting the US, Hong Kong, Taiwan, and the Philippines.

[12] "Russian Submarines Are Lurking near the Underwater Cables That Power the Internet." *Big Think*, September 30, 2021. https://bigthink.com/politics-current-affairs/russian-submarines-are-lurking-near-the-underwater-cables-that-power-the-internet/.

[13] "Team Telecom Recommends That the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States." *The United States Department of Justice*, June 17, 2020. https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.

In a 2017 submission to the US government, the parties stated that this would be the first-ever underwater infrastructure to carry information straight from Hong Kong to USA at 120 gigabytes/second. However, the administration had major security fears regarding the Chinese-owned Hong Kong corporation. According to some sources in August 2020, Google and Facebook had already installed thousands of kilometres of cabling and invested millions. Officials believed Beijing might interrupt the cable and use it for espionage purposes. Furthermore, the executive branch approved a temporary six-month deal that permitted the Taiwanese portion of the cable to proceed, but only after Google and Facebook had halted the Hong Kong connection. With increased focus on Chinese telecommunications, Facebook and Google is going to undoubtedly face more government scrutiny. This might be the first instance where the US put its foot down on a network infrastructure on security grounds. Tensions between United States and China are escalating in other area, even though they are primarily political in nature. However, Facebook and Google's experience connected to complex enterprise is only one component of a broader puzzle: the on-ground network capabilities, which is becoming an increasingly important aspect of geopolitical collaborative partnerships over the Internet.[14]

Conclusion

The 2008 Egypt case is testimony to the fact that loss of bandwidth can have disastrous impacts on human activity; a reduction in bandwidth can have the same impact on time-sensitive messages as total network failure. Owing to the inevitable consequences of network breakage, the capacity to safeguard the underwater infrastructure will become extremely crucial in upcoming wars. During the time of crisis, the attacker might launch a series of coordinated cable strikes to use them to cut off the opponent's military communications and intelligence services. Attacks against communication networks can be incredibly disruptive, as it can prohibit a nuclear-powered adversary from supervising its weapons and early-warning infrastructure.

Technological developments are expanding the danger to underwater infrastructure. However, the same developments may be used by governments to function as a safeguarding

[14] Sherman, Justin. "The US-China Battle over the Internet Goes under the Sea." *Wired*., June 24, 2020. https://www.wired.com/story/opinion-the-us-china-battle-over-the-internet-goes-under-the-sea/.

mechanism. Thanks to recent technological advancements, Unmanned Underwater Vehicles (UUVs) could be able to run unrefueled over months without interruption. Inspecting transmission lines for damage or falsification, attempting to attack enemy submarine cables and related mechanisms, keeping tabs near potentially dangerous submarines, or mobilizing payloads on the sea are just some of the key missions that could be carried out. However, commanders will be hesitant to entrust high level responsibilities to a machine. The UUV infrastructure will be required to work along with submarines or check-in with commanders for tasks that need a human decision-maker.

Acoustic communications are becoming more capable of operating across operationally significant distances with low bandwidth, whereas lasers and LEDs can attain data rates comparable to wired systems over shorter distances. A young crop of seabed systems is being developed to address the constraints of underwater communications and UUV durability. The Forward Deployed Energy and Communications Outpost (developed by the US Navy) is a box-sized device that be installed on in the ocean to serve as a supplementing rest spot for UUVs, allowing them to receive data and send commands while at the same time recharging their power. The device will allow UUVs to perform long-term activities like surveillance and inspection of cables, as well as listening for opponent submarines in SSBN patrolling regions.[15]

The future of underwater competition

As new computing and sensing technologies becomes more widely available, so does undersea knowledge and information. Over the next two decades, the race to closely monitor the underwater environment will intensify. UUVs will progressively replace submarines in undersea warfare. For tactical operations near to enemy coasts such as assaulting the opponent's underwater infrastructure, large, unmanned vehicles as well as other deployable systems that are small and less obvious might be used to a greater extent than human submarines. Soon, high-quality UUVs and seafloor sensors would be required for long-term monitoring underwater cables.

[15] "Threats to Undersea Cable Communications - Dni.gov." Accessed December 11, 2021. https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf.

There will be a race to deploy systems to the ocean's bottom, such as equipment for fast scanning and analyzing the seabed. Countries with greater underwater terrain capabilities are more likely to gain an advantage in a confrontation, especially in the early stages, when a strike on undersea cables or ballistic-missile submarines might be immensely disruptive. Predictability is essential in international relations, as is the capability of the targets to notice assaults effectively. The lack of surveillance information as well as hazards to ballistic-missile submarines' "second strike" nuclear capabilities threaten to displace today's relative stability. To maintain the utmost stability, developed nations will have to strengthen their abilities to manage the international waters tactically, just as they do in the airspace.[16]

[16]"Undersea Cables and the Future of Submarine Competition." Taylor & Francis. Accessed December 11, 2021. https://www.tandfonline.com/doi/full/10.1080/00963402.2016.1195636.