The Washington Quarterly

ISSN: 0163-660X (Print) 1530-9177 (Online) Journal homepage: www.tandfonline.com/journals/rwaq20

Protecting Undersea Cables and South Korea's Role

Amy Paik

To cite this article: Amy Paik (2025) Protecting Undersea Cables and South Korea's Role, The Washington Quarterly, 48:2, 77-91, DOI: 10.1080/0163660X.2025.2518647

To link to this article: https://doi.org/10.1080/0163660X.2025.2518647

Published online: 07 Jul 2025.

Amy Paik

Protecting Undersea Cables and South Korea's Role

The growing frequency of high-profile undersea cable disruptions—including the 2018 Africa Coast to Europe (ACE) cable blackout that affected West Africa[1] and a series of suspected attacks in 2024 involving Taiwan, Saudi Arabia, and parts of Europe[2]—have exposed the extent to which global connectivity hinges on the integrity of undersea cables and their vulnerabilities. Modern undersea cables use fiber-optic technology which transmits data at the speed of light. These cables can download high-definition movies in less than eleven minutes, making them incredibly efficient for high-bandwidth applications. (By comparison, satellite communication takes about one and a half hours to download the same high-definition movie.)[3] While satellites provide coverage in remote areas, they handle only about 3 percent of global internet traffic due to higher latency, lower bandwidth, and higher costs.

Undersea cables carry over 97 percent of the world's internet traffic

The efficiency and price competitiveness of undersea cables has prompted their widespread adoption as the primary method of global data transmission.[4] These fiber-optic systems carry over 97 percent of the world's internet traffic and support over a trillion dollars in daily financial transactions.[5] Currently, there are 574 active cables worldwide laid 8,000 miles below sea level.[6] As essential conduits for personal, corporate, and government data, undersea cables have become prime targets in a new era of hybrid warfare, where physical sabotage and cyber-enabled espionage converge.

Amy Paik is a recipient of the 2024-2025 Wilson International Competition Fellowship from the Wilson Center. She holds a doctorate of international affairs from Johns Hopkins University School of Advanced International Studies (SAIS). She can be reached by email at paikminjung@naver.com.

The Washington Quarterly • 48:2 pp. 77–91
https://doi.org/10.1080/0163660X.2025.2518647

Despite their strategic significance, undersea cables remain insufficiently protected. Recent UN General Assembly resolutions fall short of addressing the complexities of modern threats.[7] As with nuclear deterrence and arms control, a robust and enforceable international legal regime is essential to establishing norms, deterring malicious actions, and coordinating global response to threats against undersea cable infrastructures. Under the current international legal regime, the 1982 United Nations Convention on the Law of the Sea (UNCLOS) lacks enforceable provisions for surveillance, deliberate damage, and sabotage in international waters, where jurisdiction to punish the perpetrator effectively is missing.

This article reviews increasing cases of undersea cable sabotage, assesses the current gaps in international law, and proposes legal reforms. Drawing from legal documents and expert analyses, the article argues that international law must evolve to reflect technological advancements and geopolitical realities, particularly considering state-sponsored interference and increasing military interest in undersea infrastructure. In particular, it emphasizes the need for stronger global norms and binding mechanisms that secure this infrastructure against kinetic attacks and data interception.

It also contends that South Korea—home to one of the world's largest fiber-optic cable manufacturers[8]—is well-positioned to spearhead efforts in advancing undersea cable governance. Against the backdrop of intensifying US-China rivalry in the digital and maritime domains,[9] South Korea can promote a multilateral framework which balances security, sovereignty, and the global public interest in resilient internet infrastructure underseas.

The Strategic Significance of Undersea Cables

Why do undersea cables matter? Cyberspace—the global network of computer communication infrastructures which relies on undersea cables and satellites—is recognized as the fifth domain of warfare alongside land, sea, air, and space.[10] Cyberspace cannot operate in isolation, and relies heavily on the maritime domain through undersea cables for efficient data transmission between continents. Government leaders increasingly recognize that severe damage to undersea cables can shut down internet access, causing extreme disruption and financial harm.

Because of their critical importance to secure communication and financial transactions, undersea cable sabotage can serve as a weapon in the arsenals of powers looking to harm their strategic rivals. NATO has warned that Russia might target infrastructure like undersea cables to "disrupt Western life and exert pressure on countries supporting Ukraine."[11] Additionally, undersea cable

ownership gives countries and private firms power over global communication, and competition is already underway among public and private interests to invest in this technology. Currently, undersea cable ownership share represents a key facet of US-China high technology competition. In 2012, Chinese ownership of undersea cables comprised only about 7 percent of the world market, but by 2019 it had risen to 11.4 percent.[12] Its share is expected to jump to 20 percent between 2025 and 2030,[13] demonstrating China's ambition to become a world power in the undersea cable industry. This trend concerns some Western international security experts, who worry about the security of internet data which travels via these cables.[14]

Increasing Cases of Undersea Cable Disruption

Undersea cables are vital to global communications but remain susceptible to accidental damage, geopolitical conflicts, and potential sabotage. As reliance on these infrastructures grows for internet access, incidents of undersea cable sabotage have raised concerns about the absence of robust protections and enforcement mechanisms. The case studies below highlight instances of undersea cable sabotage or deliberate interference, emphasizing the economic, security, and political vulnerabilities tied to their fragility. Whether due to state-sponsored actions or unforeseen mishaps, these case studies show the pressing need for international collaboration and regulatory measures to safeguard the undersea cable infrastructure.

2018 ACE Undersea Cable Case

The media began reporting heavily on the location of undersea cables when a major cable connecting two continents was damaged in 2018, causing widespread internet blackouts. This incident quickly drew global attention, highlighting the impact of cable damage on daily life. In March, the 17,000-kilometer-long ACE cable, which links the west coast of Africa to Europe, broke, causing thirteen countries in West Africa to lose internet for two days.[15]

It remains unclear to the public whether the cut in the ACE was a deliberate attack or merely an accident. UK journalist Jim Edwards speculated in *Business Insider* that Sierra Leone could have damaged the ACE cable; at the time, its government was often blamed for disrupting cables.[16] But the responsibility for damaging the cable has yet to be determined. Whether the ACE cable case was an accident or not, it shows the consequences that people could suffer when a cut occurs. Not having internet for two days harmed people's businesses and caused major inconveniences. The incident led many world leaders to start

exploring whether any backup plan is in place to ensure internet connectivity in the case of undersea cable sabotage.[17]

2019 Losharik Submarine Case

In July 2019, experts warned that Russia was investing in and testing its submarines' capability to cut cables in hard-to-fix places.[18] A Russian media outlet, *Novaya Gazeta*, suspected the *Losharik*, a Russian nuclear-powered submarine, might have cut Norwegian undersea cables located 60 nautical miles east of Norway.[19] The *Losharik* can dive up to 20,000 feet, ten times deeper than the operating depth of forty-five human-crewed US submarines.[20] The Russian Defense Ministry's official position in 2019 was that a fire happened on the *Losharik* while the vessel measured the seabed's depth and damaged the cables by accident. Regardless, this was the first worldwide suspected case of Russian disruption of undersea cables. One can argue from this incident that Russia may be on the path to using its technology to sever cables more openly—Russia's "shadow fleet" activity is no longer in the shadows.[21]

2023 Matsu Island Case

On February 2 and 8, 2023, the cables linking Taiwan and the Matsu Islands were damaged twice, causing an internet blackout for 13,000 Matsu Island residents. After fifty days, the undersea cables were repaired. Taiwan attributed the incident to Chinese ships, highlighting the serious concerns surrounding intentional or accidental cable sabotage.[22] Elizabeth Braw, a national security expert from the American Enterprise Institute, commented that some still suspect Chinese vessels deliberately cut the undersea cables. She observed that consecutively experiencing the loss of two undersea cables is highly uncommon, meaning this was either an exceedingly unlucky event or more than mere chance.[23] It is complex to assign blame, which is why the international regime is behind in effectively punishing perpetrators, but the longer we wait, the more serious the problem becomes.

It is complex to assign blame, but the longer we wait, the more serious the problem becomes

2024 Red Sea Cases

On February 7, 2024, the BBC reported that the Houthis shared a plan through the Telegram messaging app to target undersea cables linking Europe and Asia in the Red Sea.[24] The same day, *Foreign Policy* magazine staff writer Keith Johnson

wrote that if the Houthis currently lacked the capability, Iran might assist them by providing assets.[25] These forecasts materialized in under a month. On February 26, 2024, four undersea cables connecting Saudi Arabia and Djibouti were assaulted, disrupting internet communications and causing delays and possible information leaks.[26]

Then, on November 17, a cable in the Red Sea connecting Lithuania and Sweden was also disrupted. The next day, another cable disruption occurred on a cable connecting Germany and Finland. A Chinese vessel, *Yi Peng 3*, was found nearby both incidents, but this may not be enough evidence to hold China accountable.[27] The Danish navy caught *Yi Peng 3* in the straits between Denmark and Sweden after the second incident. The Swedish coast guard got involved with the investigation after learning that the damage both times happened in Sweden's exclusive economic zone (EEZ).[28] Still, the challenge remains to prove that this was an intended attack by China, not a vessel trespassing by accident.

Developing Legal and Security Frameworks

What the above cases reveal is that establishing long-term infrastructural stability for undersea cables will require strengthening international law, as well as multilateral military and intelligence partnerships. The following sections discuss recent developments in the UN, the G7, and military and diplomatic initiatives—and opportunities for improvement through these venues.

Legal Gaps in UNCLOS for Cable Protection

In international waters, Article 113 of the UN Convention on the Law of the Sea (UNCLOS) obliges states to adopt laws criminalizing international damage to undersea cables. However, when a cable is damaged in international waters, the jurisdiction to hold the perpetrator accountable does not fall to the owner of the cable under the current regime. Instead, even if the ship that caused the damage gets identified, the courts of the ship owner's country or the nationality of the captain deals with the case, not the courts of the cable owner's country. Additionally, UNCLOS does not explicitly grant the right to board vessels or arrest people suspected of cable damage.[29] Because of this, there has not been a case where a cable cut has gone to the courts. Experts fear that states don't change international law on this issue proactively because on some grounds, state actors are suspected to be behind undersea cable sabotages. Therein lies the problem: the law exists but cannot be effectively enforced due to the jurisdictional structure.

In 2023, a new resolution on the Ocean and the Law of the Sea was passed by the United Nations General Assembly (UNGA).[30] However, this resolution simply reiterated the provisions of UNCLOS concerning the undersea communication cables without introducing any new elements. The same applies to undersea pipelines, which transport oil and gas, in international waters. Despite the rulings that something must be done and the resolutions that were issued, there have been no concrete changes and our information remains vulnerable. States are supposed to protect individuals and countries' national security, but in the current situation, states are not taking responsibility to protect individuals internationally. They could make the law more effective, but the international will is unavailable.

As stated, the UN General Assembly (UNGA) Resolution on Oceans and the Law of the Sea reiterated what was previously stated in UNCLOS. Specifically, the resolution "recognizes that submarine cables and pipelines are vitally important to the global economy and the national security of all states, conscious that these cables and pipelines are susceptible to intentional and accidental damage and calls upon states to take measures to protect submarine cables and pipelines and to fully address issues relating to these cables and pipelines, in accordance with international law, as reflected in the Convention."[31] Additionally, it "encourages states' adoption of laws and regulations necessary to provide that the breaking or injury or conduct calculated or likely to result in such breaking or injury of submarine cables or pipelines beneath the high seas done willfully or through culpable negligence shall be a punishable offence, and further calls upon states to enforce such laws against ships flying their flags or a person subject to their jurisdiction, in accordance with international law, as reflected in the Convention."[32]

My suggestion is to improve the provisions in the 2023 UNGA Resolution on Oceans and Law of the Sea by including the following idea: The court of the country of the cable owner's citizenship should be open to civil actions brought by the owner against someone, who allegedly damaged that cable, regardless of any other connection that the defendant might have to that jurisdiction. The country of the cable owner's citizenship should be permitted to prosecute the party alleged to have caused the damage in its domestic courts, as UNCLOS provided in the perpetrator's court. These proposed revisions aim to strengthen international legal protection for undersea cables and the data they carry by addressing jurisdictional gaps in international waters. They call for clearer civil

The country of the cable owner's citizenship should be permitted to prosecute in its courts

remedies and more precise legal language, surpassing the UNGA resolution. Additionally, they advocate for expanding the scope for prosecution to be beyond the perpetrator's jurisdiction to include that of the cable owner, enhancing deterrence and reducing the likelihood of intentional cable damage.[33]

The Role of the G7

Starting in 2022, undersea cables were mentioned in the G7 Communique as part of the core agenda. That year, members (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States) pledged to "strengthen our efforts to facilitate data flow with trust across borders."[34] The wording was vague but thought-provoking.

What "data flow with trust across borders"[35] meant became more explicit in the following year's communique, which called for "like-minded partners … extending undersea cable routes with secure cables to stay together." Here, the like-minded partners meant the G7 countries, who signed the communique together in 2022. This showed the United States' firm determination to never share its cables with untrusted companies—but its willingness to share with "like-minded" countries such as the G7 powers. The states that believe in democracy were coming forward, declaring their plan to stay together when they make a consortium and invest in establishing critical infrastructures such as communication cables.

A year later, the May 2023 G7 summit in Hiroshima concluded with a communique containing a section on undersea cables.[36] This included discussion of enhancing network resilience with like-minded partners by extending secure routes for undersea cables. The G7 Hiroshima Leaders' Communique likely resulted from increasing threats to global network infrastructures.[37] When the G7 Communique 2023 discussed the need to work with trusted states to better protect undersea cables, the wording became more specific, shifting from the 2022 Communique's call for "like-minded" partners to a call for "open democracies," stressing the need for democratic countries to work together.

In the 2024 G7 Communique, a paragraph was also dedicated to undersea cables, which stated that "We will … advance our cooperation on secure and undersea cable connectivity, particularly for strategic routes such as the Arctic and the Pacific." Here, their vision to better coordinate "technical security requirements and advancing research on the economic and environmental sustainability of cable connectivity" is shared.[38] The latest communique sounds like an implementation plan from the earlier communique from G7 states on how democratic nations are willing to work side by side and invest together in the less cable-dense parts of the region, such as the Arctic and the Pacific,

making sure that their "secure" undersea cable infrastructure is present instead of those from China and its partner nations. From my perspective, the rhetorical evolution across these communiques demonstrates a growing tangible commitment by the G7 to translating strategic intentions into actionable steps, marking a productive shift from mere declarations to substantive efforts in securing critical infrastructure, at least in the area of investing in the undersea cable infrastructure together.

Military and Diplomatic Initiatives

Since last year, multilateral military and intelligence efforts have been mobilized to safeguard cable infrastructure. For instance, the Nordic Warden operation, initiated in 2024, leverages AI-driven surveillance to counter Russian interference with undersea cables in the Baltic Sea. Ten nations—Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, the Netherlands, Norway, Sweden, and the UK—operate together in the Nordic Warden under UK leadership.[39]

The United States has also sought to enhance international cooperation in better guarding undersea cables. A December 2024 white paper released by the Office of Economic Security, the Supply Chain Resilience Center, and the Cyber Security and Infrastructure Security Agency pledged that the US government will create opportunities to perform joint exercises with other countries or even the private sector.[40] For example, opportunities to harmonize the real-time situational awareness and incident information-sharing between governments, allies, and private sector stakeholders are now being identified.[41] Although this document was published during the Biden administration, the Trump administration, concerned about China's threat to US security, is unlikely to pull back on this agenda.

South Korea's Potential Leadership Role

For South Korea, the undersea cables issue represents an opportunity to take a leading role in fostering international cooperation and progress, aligning with the country's goal to become a "global pivotal state."[42] South Korea's Global Pivotal State (GPS) vision, introduced by former President Yoon Suk Yeol, is a strategic foreign policy approach advocating for a broader international role for South Korea beyond the Korean Peninsula. Initially outlined during his 2022 presidential campaign, the concept emphasizes South Korea's contribution to global stability, economic prosperity, and democratic principles. While drawing from past initiatives like former President Lee Myung-bak's "Global Korea" policy, the GPS vision aspires to establish a more proactive and influential South Korean global presence.

Given the current geopolitical landscape, South Korea is uniquely positioned to spearhead international initiatives aimed at safeguarding undersea cable infrastructure. Its cutting-edge fiber-optic technology, substantial investments in maritime connectivity, and strategic partnerships with Western nations enhance its leadership potential in this domain. As concerns mount over potential threats from China, Russia, and North Korea, South Korea's proficiency in cybersecurity and maritime infrastructure underscores its role as a vital contributor to strengthening international norms for undersea cable security. Additionally, its geographic location in East Asia allows it to reinforce regional stability alongside the United States and Japan while serving as a strategic counterweight to China's expanding influence.

South Korea is uniquely positioned to spearhead efforts to safeguard undersea cables

Incorporating South Korea into strategic alliances like AUKUS or other Western-led initiatives would enable G7 nations to bolster deterrence, safeguard essential communication networks, and mitigate reliance on adversarial states for digital infrastructure. Ultimately, South Korea's leadership in this field would help ensure a resilient and independent global communication network that reinforces both economic and security interests.

Growing Momentum

In South Korea, the discussion over the importance of guarding the undersea cable infrastructure has gained momentum. In 2024, the Sejong Institute, one of the three prominent think tanks in South Korea, organized two seminars dedicated to the topic of undersea cable sabotage in May and August of 2024.[43] Dr. Sung Won Lee, director of the Center for Security and Strategy at Sejong Institute, reported that members of the South Korean Coast Guard, the Ministry of Defense, and the Ministry of Foreign Affairs were all greatly concerned about the operational fitness of nine active South Korean cables, which led them to participate with great interest in a scenario-based exercise to check South Korea's preparedness in the case of an intended attack on the undersea cable infrastructure.[44] Traditionally, former officers attend such meetings; persuading sitting officers—active officers with current positions—to participate is rare unless the topic is timely and important.

Leveraging UNGA Engagement

Building on this growing momentum in South Korea, Foreign Minister Tae-yul Cho addressed the UN General Assembly in September 2024, pledging that South Korea would seek to act as a facilitator, supporter, and initiator for global

peace, development, and the charting of new norms and governance for new technologies.[45] Additionally, at the 79th annual UNGA in New York in September 2024, the United States and its allies—including South Korea—issued the "New York Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World" (also known as the New York Joint Statement).

The statement highlights the critical importance of protecting undersea communication networks. It emphasizes the need for policies ensuring the resilience, security, and efficiency of undersea cables while maintaining global interdependence despite emerging threats such as sabotage.[46] This latest statement—its efficacy likely bolstered by US participation—shows that more states are cooperating on safety concerns regarding undersea cable data. However, it is important to point out that not all US allied nations, or even all G7 nations, decided to join this principle. With remaining opportunities to bring new global actors into the fold, South Korea can leverage its expertise as one of the world's leading fiber-optic cable suppliers to suggest changes to international laws regulating undersea cables.

Collaborating with International Organizations

By collaborating with other nations and organizations such as the International Telecommunication Union (ITU) and the International Maritime Organization (IMO), South Korea has successfully ensured the security of its own undersea cable providers, reduced latency, and enhanced route diversity while developing ideas to guard cables from intentional and unintentional sabotage.[47] Moving forward, South Korea can collaborate with the IMO to advocate for establishing international standards for overseeing undersea cables—even beyond its territorial waters. Reexamining the reform of IMO rules and regulations to safeguard undersea cables better is another crucial matter to address. The IMO can set agendas and inspire nations to establish international norms,[48] building on its eight-year leadership through former Secretary General Kitack Lim, who was from South Korea.

South Korea can also exercise policy influence by working with the ITU to promote undersea cable protection and advocate for their broader use as a public good for monitoring climate change. This possibility is highlighted in a 2010 ITU publication, which confirms that these cables can perform various climate-related functions such as monitoring environmental changes.[49] In this context, South Korea could advocate for the broader use of cables as a reason to consider undersea communication cables a public good. South Korea can also seek to join the G7 as a permanent member and start working on cosponsoring undersea cable projects with other democratic nations such as Australia, Japan, and the United States.[50]

Cosponsoring Undersea Cable Projects

In June 2023, the East Micronesia Cable (EMC) project, valued at $95 million USD and funded by Australia, Japan, and the United States, commenced as a model of international cooperation. This initiative aims to construct undersea cables in the Pacific, delivering high-quality, secure, and reliable internet to Pohnpei, Kosrae, Tarawa, and Nauru. It is a significant milestone as the first undersea cable providing more secure, high-quality digital access to these four islands, including those in the Federated States of Micronesia.

This model project exemplifies these countries' joint efforts to help a less affluent part of the world by subsidizing a core infrastructure for communication, the EMC.[51] Additionally, it exemplifies how like-minded powers can coordinate on initiatives to counter China's increasing control over the world's undersea cables and establish equitable control of this communication infrastructure.[52] Learning from the EMC project, South Korea can join these efforts with Australia, Japan, and the United States, which are collectively working to counter Chinese influence in building the critical infrastructure of undersea cables in the Pacific.

The Path Forward

The lack of comprehensive international regulations to address risks surrounding undersea cables leaves critical infrastructure vulnerable to sabotage. Without laws to hold perpetrators accountable, diplomatic efforts alone are insufficient to deter such attacks. Despite the challenges of revising the UNCLOS,[53] it remains urgent to achieve an effective international regime, as intentional sabotage can expose sensitive data including financial transactions and communication records. While tensions over undersea cable ownership intensify between the United States and China, nations continue seeking solutions to prevent sabotage and safeguard global connectivity.

Without laws to hold perpetrators accountable, diplomatic efforts are insufficient

South Korea, the fourth-largest supplier of fiber optic cables globally,[54] can play a key role in advancing undersea cable protection. The nation has signaled its commitment to international collaboration, including signing agreements with the UN and supporting the Resolution on Oceans and the Law of the Sea. Additionally, South Korea aims to expand its leadership role in global organizations such as the G7 and the UN General Assembly in line with its GPS vision.

South Korea could contribute to safeguarding undersea cables and bolstering international norms by cosponsoring projects with countries such

as the United States and Japan. Undersea cables are unlikely to lose attention in South Korea, as they remain a critical matter of national security and protecting them has bipartisan support. South Korea, in sustained collaboration with other nations, should continue to safeguard and prioritize this essential policy area.

Notes

1. Jim Edwards, "The Internet's Worst-case Scenario Finally Happened in Real Life: An Entire Country Was Taken Offline, and No One Knows Why," *Business Insider*, April 10, 2018, https://www.businessinsider.com/undersea-international-internet-cables-cut-in-africa-2018-4.
2. Frank Gardner, "Could the Houthis Sabotage Undersea Cables?" BBC, February 7, 2024, https://www.bbc.com/news/world-middle-east-68231945; Elizabeth Braw, "China is Practicing How to Sever Taiwan's Internet: The Cutoff of the Matsu Island May Be a Dry Run for Further Aggression," *Foreign Policy*, February 21, 2023, https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/; Rob Schmitz, "Sabotage Suspected after Undersea Cables Damaged in the Baltic Sea," *All Things Considered* (podcast), NPR, November 20, 2024, https://www.npr.org/2024/11/20/nx-s1-5197701/underwater-telecom-cables-in-the-baltic-sea.
3. J. Dahm, "Undersea Fiber-optic Cable and Satellite Communications: A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea," Johns Hopkins Applied Physical Laboratory, December 2022, https://www.jhuapl.edu/sites/default/files/202212/UnderseaFiberOpticCableandSATCOM.pdf.
4. David Schafer, "Satellite Internet vs. Cable Internet," Satellite Internet, July 18, 2023, https://www.satelliteinternet.com/resources/satellite-internet-vs-cable-internet/.
5. J. S. Van Oudenaren, "Submarine Cables: Backgrounder for Maritime Awareness Project," National Bureau of Asian Research, July 2018, https://map.nbr.org/2018/07/submarine-cables/.
6. Dave Reynolds, "Undersea Cables Keep Us Connected," Share America, June 11, 2024, https://share.america.gov/undersea-cables-keep-us-connected/.
7. Amy Paik, "Building an International Regulatory Regime in Submarine Cables and Global Marine Communications," Johns Hopkins University ProQuest, 2022, https://www.proquest.com/openview/eddd5e64f7a53595ab958126e158c4c8/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y.
8. EBS Documentary, "Korea Ranks 4th in the World: Korea's First Submarine Cable Installation Site," Youtube, 2023, https://www.youtube.com/watch?v=kyaZl_wBoU8.
9. Dan Smith et al., "China and the US Are Wrestling over a Web of Cables We Never See but Rely on Every Day," ABC News, March 6, 2024, https://www.abc.net.au/news/2024-03-06/the-cloud-under-the-sea/103137378; Jonathan E. Hilman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 2021); Stewart M. Patrick and guest blogger for *The Internationalist*, "Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road," *The Internationalist*, July 2, 2024, https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road.

10. Andrea Little Limbago, "One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft," Eurasia Review, August 20, 2015, https://www.eurasiareview.com/20082015-one-size-does-not-fit-all-the-multifaceted-nature-of-cyber-statecraft-analysis/.
11. Charlie Cooper, "NATO Warns Russia Could Target Undersea Pipelines and Cables," POLITICO, May 3, 2024, https://www.politico.eu/article/nato-warns-russia-could-target-undersea-pipelines-and-cables/.
12. Azhar Azam, "The Geopolitics of Cables: US and China's Subsea War," Fair Observer, December 17, 2024, https://www.fairobserver.com/politics/the-geopolitics-of-cables-us-and-chinas-subsea-war/#.
13. Raghvendra Kumar, "Securing the Digital Seabed: China's Underwater Ambitions," *Journal of Indo-Pacific Affairs*, November 14, 2023, https://media.defense.gov/2023/Nov/14/2003340185/-1/-1/1/FEATURE%20KUMAR%20-%20JIPA.PDF.
14. J. S. Van Oudenaren, "Submarine Cables: Backgrounder for Maritime Awareness Project," National Bureau of Asian Research, July 2018, https://map.nbr.org/2018/07/submarine-cables/.
15. Edwards, "The Internet's Worst-case Scenario."
16. *Ibid*.
17. Stew Magnuson, "Sensors, AI Possible Solutions to Preventing Undersea Cable Sabotage," *National Defense*, May 13, 2025, https://www.nationaldefensemagazine.org/articles/2025/5/13/sensors-ai-possible-solutions-to-preventing-undersea-cable-sabotage.
18. H. I. Sutton, "How Russian Spy Submarines Can Interfere with Undersea Internet Cables," *Forbes*, August 19, 2020, https://www.forbes.com/sites/hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/.
19. Nikolai Litovkin, "Everything Known about the Top Secret 'Losharik' Submarine," Russia Beyond, July 3, 2019, https://www.rbth.com/science-and-tech/330607-everything-known-about-losharik.
20. James Glanz and Thomas Nilsen, "A Deep-diving Sub, a Deadly Fire, and Russia's Secret Undersea Agenda," *New York Times*, April 21, 2020, https://www.nytimes.com/2020/04/20/world/europe/russian-submarine-fire-losharik.html.
21. Frontier India News Network, "From WWI to Today: The Hidden History of Undersea Cable Warfare," *Frontier India*, March 28, 2025, https://frontierindia.com/from-wwi-to-today-the-hidden-history-of-undersea-cable-warfare/.
22. Wen Lii, "After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communication Resilience." The Diplomat, April 15, 2023, https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/.
23. Elizabeth Braw, "China is Practicing How to Sever Taiwan's Internet: The Cutoff of the Matsu Island May Be a Dry Run for Further Aggression," *Foreign Policy*, February 11, 2023, https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/.
24. Frank Gardner, "Could the Houthis Sabotage Undersea Cables?" BBC, February 7, 2024, https://www.bbc.com/news/world-middle-east-68231945.
25. Keith Johnson, "The Houthis' Next Target May be Underwater," *Foreign Policy*, February 7, 2024, https://foreignpolicy.com/2024/02/07/houthi-red-sea-attacks-submarine-cables/; Kali Robinson, "Iran's Support of the Houthis: What to Know," Council on Foreign Relations, March 24, 2025.
26. "Houthis Knock out Underwater Cables Linking Europe to Asia," *The Jerusalem Post*, February 26, 2024, https://www.jpost.com/middle-east/article-788888; Assaf Gilead,

"Houthis Hit Submarine Communication Cables," Globes, February 26, 2024, https://en.globes.co.il/en/article-houthis-hit-underwater-communications-cables-1001472165.
27. Elizabeth Braw, "Suspected Sabotage by a Chinese Vessel in the Baltic Sea Speaks to a Wider Threat," Atlantic Council, November 21, 2024.
28. Schmitz, "Sabotage Suspected after Undersea Cables Damaged in the Red Sea."
29. United Nations, "United Nations Convention on the Law of the Sea," December 10, 1982.
30. United Nations, "General Assembly Adopts Two Resolutions on Oceans, Highlighting Mounting Threats to Marine Resources, Need to Tackle Rising Sea Levels to Tackle Risky Sea Levels, Damage to Ecosystems," December 5, 2023, https://press.un.org/en/2023/ga12569.doc.htm#:~:text=Adopting%20resolution%20"Oceans%20and%20the%20law%20of%20the,and%20the%20vital%20importance%20of%20preserving%20its%20integrity.
31. United Nations General Assembly, "Oceans and the Law of the Sea," A/78/L.15, November 28, 2023, paragraph 175, https://documents.un.org/doc/undoc/ltd/n23/369/28/pdf/n2336928.pdf?OpenElement&_gl=1*1ge1qoi*_ga*NjQ3ODEyNDY1LjE3NDg5NzQyMDQ.*_ga_TK9BQL5X7Z*czE3NDg5NzQyMDQkbzEkZzEkdDE3NDg5NzQ1MTEkajYwJGwwJGgw.
32. *Ibid.*, paragraph 177.
33. Amy Paik, "South Korea: A Catalyst for Fixing Laws on Undersea Cables," The Peninsula Blog, Korea Economic Institute, March 8, 2024, https://keia.org/the-peninsula/south-korea-a-catalyst-for-fixing-laws-on-undersea-cables/
34. Hannah Grothusen et al., "G7 Hiroshima Summit Outcomes," Center for Security and International Studies, May 23, 2023, https://www.csis.org/analysis/g7-hiroshima-summit-outcomes.
35. Roundtable of G7 Data Protection and Privacy Authorities, "Communique: Promoting Data Free Flow with Trust and Knowledge Sharing about the Prospects for International Data Spaces," September 8, 2022, https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2022/communique-g7-220908/
36. The White House, "G7 Hiroshima Leaders' Communique," 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communique/.
37. Taijing Wu and Firstinitial Lai, "Taiwna Suspects Chinese Ships Cut Islands' Internet Cables," Associated Press, April 18, 2023, https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70.
38. The White House, "Apulia G7 Leaders' Communique," June 14, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/14/g7-leaders-statement-8/.
39. George Allison, "Britan Launches AI System to Monitor Russian Shadow Fleet," UK Defense Journal, January 6, 2025, https://ukdefencejournal.org.uk/britain-launches-ai-system-to-monitor-russian-shadow-fleet/.
40. US Department of Homeland Security, "Priorities of DHS Engagement on Subsea Cable Security & Resilience: A White Paper by the Office of Economic Security, the Supply Chain Resilience Center, and the Cyber Security and Infrastructure Security Agency," December 24, 2024, https://www.dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf.
41. Anna Ribeiro, "US, Nordic-Baltic Allies Focus on Undersea Cable Security Amid Cyber Incidents as NATO Begins Baltic Sea Mission," Industrial Cyber, January 20, 2025,

https://industrialcyber.co/threat-landscape/us-nordic-baltic-allies-focus-on-undersea-cable-security-amid-cyber-incidents-as-nato-begins-baltic-sea-mission/
42. Andrew Yeo, "South Korea as a Global Pivotal State," Brookings Institute, December 19, 2023.
43. "KDI, Economic and Industrial Think Tank 'No. 1 for 8 Consecutive years … IFANS also 'Leads on the Top for 12 Years," Hankyung Business, 2020, https://magazine.hankyung.com/business/article/202003313694b.
44. "Sejong Institute Tabletop Exercise," Sejong Institute, 2024, https://www.sejong.org/web/boad/1/egoread.php?bd=60&itm=&txt=&pg=1&seq=7731.
45. "Remarks by H.E. Cho Tae-yul, Minister for Foreign Affairs at the General Debate of the General Assembly's Seventy-ninth Session," America Times News Service, 2024, https://www.america-times.com/remarks-by-h-e-cho-tae-yul-minister-for-foreign-affairs-of-the-republic-of-korea-at-the-general-debate-of-the-general-assemblys-seventy-ninth-session/.
46. US Department of State, "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World," 2024, https://www.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/.
47. "South Korea Takes the Lead in Protecting Undersea Cables: Urgent Need for International Regulation," Public Law Library, 2024, https://publiclawlibrary.org/south-korea-takes-the-lead-in-protecting-undersea-cables-urgent-need-for-international-regulation/.
48. "Estonia Pushes for Maritime Law Reforms to Safeguard Undersea Cable Infrastructure," Ship Universe, December 27, 2024, https://www.shipuniverse.com/news/estonia-pushes-for-maritime-law-reforms-to-safeguard-undersea-infrastructure/.
49. "Using Submarine Communications Networks to Monitor the Climate," Yuzhu You of the Institute of Marine Science, University of Sydney, Australia, November 20, 2010, https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000110003PDFE.pdf.
50. Victor Cha and John J. Hamre, "A Reimagined G7," Center for Strategic and International Studies, June 14, 2024, https://www.csis.org/analysis/reimagined-g7.
51. US Department of State, "Joint Statement on Improving East Micronesia Telecommunications Connectivity," 2021, https://www.state.gov/joint-statement-on-improving-east-micronesia-telecommunications-connectivity/.
52. Kent Calder, "Cable Wars: What to Do about Deepening Conflict beneath the Seas?" Asia Times, April 11, 2025, https://asiatimes.com/2025/04/cable-wars-what-to-do-about-deepening-conflict-beneath-the-seas/.
53. Amy Paik, "Building an International Regulatory Regime in Submarine Cables and Global Marine Communications," Johns Hopkins University ProQuest, 2022, https://www.proquest.com/openview/eddd5e64f7a53595ab958126e158c4c8/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y.
54. EBS Documentary, "Korea Ranks 4th in the World."