CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

DECEMBER 2024

THE GEOPOLITICS OF SUBSEA DATA CABLES

Securing Europe's Subsea Data Cables

Sophia Besch and Erik Brown

Securing Europe's Subsea Data Cables

Sophia Besch and Erik Brown

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Introduction

More subsea data cables connect to Europe than to any other continent around the world. But it was not until 2022 that European policymakers began to pay significant attention to the security of these cables. Russia's invasion of Ukraine, as well as a subsequent series of incidents resulting in damages to European undersea infrastructure, raised alarm bells in Brussels and beyond. The Nord Stream explosion in fall 2022 and the Balticconnector gas pipeline incident just over one year later illustrated the glaring vulnerability of Europe's undersea infrastructure to sabotage. The involvement of a Hong Kong–flagged vessel in the October 2023 Balticconnector incident also sparked awareness among Europeans of China's potential interest in physically damaging undersea infrastructure in and near Europe. Most recently, in mid-November 2024, two undersea data cables—connecting Finland and Germany and Sweden and Lithuania, respectively—were damaged due to "external impact."[1]

In addition to the physical threats to Europe's undersea infrastructure, subsea cable systems and the data that flow through them are vulnerable to hacks, espionage, and other cyber risks.[2] Militaries fear a range of threats: backdoors could be installed during the cable manufacturing or repair process; cable-landing stations, where subsea cables connect to terrestrial networks, could become targets to cyber attacks, especially as control over these centers is being shifted to remotely controllable network management systems; and rapid advances in subsea technology might even allow adversaries to tap cables at sea.[3]

The North Atlantic Treaty Organization (NATO), the European Union (EU), and individual European governments have over the last three years initiated a flurry of initiatives that aim to bolster the physical security and cybersecurity of cables and other undersea infrastructure. Yet information sharing and resourcing often remains insufficient. Approaches also vary from country to country. There is not a single regulatory regime for protecting

subsea data cables.[4] Instead, there are many different regimes, national agencies, authorities, and international entities involved in the protection of this critical infrastructure, complicating a joint European approach.[5]

Fierce competition between the United States and China over subsea cables is also forcing a debate in Europe about cable ownership and integrity, especially with regard to cybersecurity and espionage concerns.[6] Partly in response to U.S. warnings, European policymakers are becoming increasingly wary of subsea cables supplied by vendors they consider high risk—chiefly those based in China.[7] The U.S. government is keen to expand its cooperation with Europeans to better expand, protect, and repair trusted subsea cable networks.[8]

At the same time, however, competition between U.S. and European firms is complicating a more joint transatlantic approach. There is some concern in Europe over the emerging dominance in new cable investment by a few U.S. "hyperscalers," or large-scale cloud providers such as Google and Meta, and what this new market dynamic might mean for European telecommunications firms. Absent a more strategic approach to building out its own digital network and providing the adequate resources to do so, Europe risks losing out in the competition between Washington and Beijing under the world's seas.

This paper's first section briefly maps the economic significance, strategic vulnerabilities, and key players of Europe's undersea cable infrastructure. It also outlines the recent evolution of the European debate on the physical and economic security and cybersecurity of subsea cables, sketching the European perspective on the activities of Russia, China, and the United States in this field. The second section describes European countries' steps—taken through NATO, the EU, and other multilateral groupings—to protect their subsea cable networks and increase their global competitiveness. The final section identifies shortcomings of current approaches and offers a list of policy recommendations to lawmakers in Europe, with a view to improving the physical security, cybersecurity, and resilience of their undersea data cables.

To obtain a clearer picture of their assets and vulnerabilities, Europeans should work together to map and review critical undersea infrastructure and improve their information-sharing mechanisms and stakeholder exchanges. To improve the security of their cables, Europeans should also invest in developing new undersea infrastructure protection technology, allocate more resources to support Europe's market leaders in subsea cable installation and repair, and work with partners to ensure secure and trusted end-to-end supply chains. Looking to the future, Europeans should strengthen digital connectivity in regions of strategic importance and creatively build out diplomatic relations with partner countries through the construction and repair of new and existing cables.

Despite the global focus in recent years on U.S.-China competition over subsea data cables, Europe possesses several advantages in this realm.[9] As the contest between China and the United States ramps up and Russia becomes ever more emboldened in its attacks on European infrastructure, Europeans must invest more to leverage these advantages and protect the competitiveness, resilience, and security of their subsea cable infrastructure.

The European Subsea Cable Ecosystem and State of Debate

Europe is home to several global industry leaders in subsea cable installation and repair. At the same time, the continent lacks peer competitors to U.S. hyperscalers that are becoming increasingly relevant in new cable investments. As incidents of cable damage and potential sabotage occur more frequently in European waters, governments across Europe are beginning to recognize the risks posed by geopolitical competitors, including China and Russia, to their critical undersea infrastructure.[10] Debates across Europe have shifted from whether more needs to be done to protect subsea cable systems to what should be done and by whom. The latter question is especially salient. Subsea data cables are vital for connectivity across the entire European continent, but they only connect to a small number of coastal states. In addition, a wide range of stakeholders are involved in the cables' functioning, but information sharing is challenging.

Economic Significance, Strategic Vulnerabilities, and Key Players

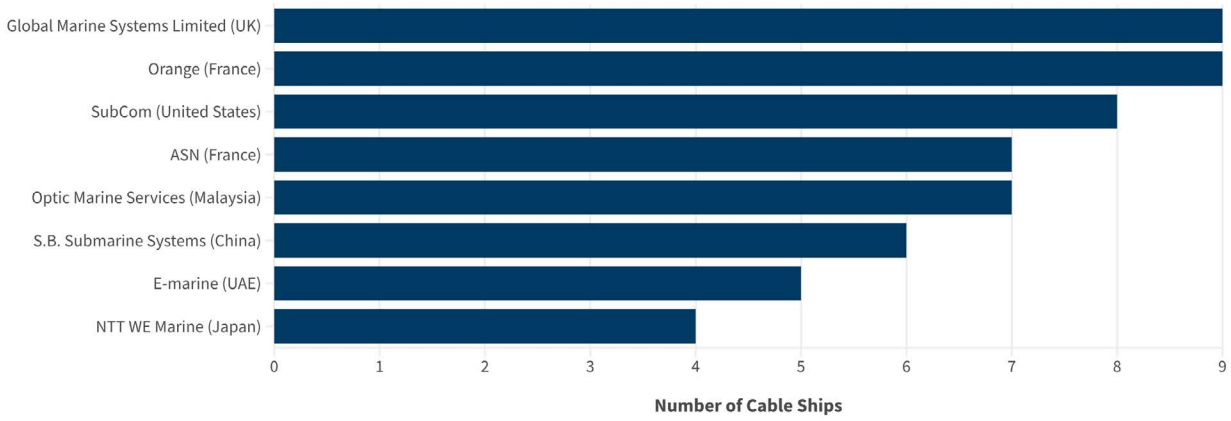
Individuals across Europe rely on the internet daily to communicate with each other and make financial transactions.[11] Of the approximately 250 active cables that ensure the EU is connected to the global internet, two-thirds are submarine cables.[12] Thus, Europe's dependence on digital connectivity is also a dependence on submarine cables. Globally, it is estimated that $10 trillion worth of financial transactions travel through these cables every day. David Cattler, a former NATO assistant secretary general for intelligence and security, rightly labelled undersea cables an "economic lynchpin."[13] In a speech at the European Parliament, Commission President Ursula von der Leyen called on European leaders to better protect the undersea cables that connect their citizens and companies to the world.[14]

The global subsea cable supplier market is dominated by four major companies, of which one is European: France's Alcatel Submarine Networks (ASN). It competes with the United States' SubCom, Japan's Nippon Electric Company (NEC), and China's HMN Technologies (or HMN Tech, formerly called Huawei Marine Networks). As of 2024, ASN is the current market leader among these major players, both in terms of new systems installed and total kilometers of cable produced from 2020 to 2024.[15] ASN also leads its competitors in the number of planned systems by supplier.[16] Other notable European subsea cable suppliers include the United Kingdom's Xtera, which produces cables and cable parts but does not provide installation or maintenance services, and Telecom Italia's Sparkle subsea cable unit. In recent months, the Italian government has shown interest in acquiring Sparkle, placing a new bid for the company after its first offer was rejected in early 2024.[17] If the offer is accepted, both the French and Italian governments would own globally prominent submarine cable suppliers (ASN and Sparkle), underscoring the increased focus placed within European capitals on these systems.[18]

While ASN is an industry leader in undersea cable installation in Europe, the continent lacks a competitor to the U.S. hyperscalers dominating new cable investment and construction. The heightened presence of these large actors threatens to push out smaller European telecommunications firms in terms of future cable planning and investment.[19] What is more, the margins of cable manufacturers such as ASN remain relatively low despite new orders pouring in from new players. In 2021, ASN's profits were approximately €4 million (nearly $4.5 million), despite its revenue doubling to just under €1 billion (or just over $1 billion) since 2018.[20]

Approximately eighty ships around the globe are responsible for laying, maintaining, and repairing the cables that run along the ocean floor. Only five companies possess seven or more ships in their cable fleet, and three of these companies are headquartered in Europe (see Figure 1).[21] France's telecommunications firm Orange and the United Kingdom's Global Marine Systems Limited are the current global leaders in cable ship ownership, each with nine ships. SubCom owns eight ships and France's ASN and Malaysia's Optic Marine Services each have a fleet of seven ships. Companies with slightly smaller fleets include China's S.B. Submarine Systems with six ships, the UAE's E-marine with five ships, and Japan's Nippon Telegraph and Telephone World Engineering Marine (NTT WE Marine) with four ships. Although there is a concentration of cable ship companies with headquarters in Europe, their vessels are sprawled across the world, either laying new cables or maintaining or repairing cables.[22]

Figure 1. Cable Ship Fleet Distribution by Company



Source: Submarine Telecoms Forum, "Industry Report, 2024–2025: Issue 13," 95.
Note: Only companies with four or more ships are included in the figure.

For most of Europe, sufficient digital connectivity redundancies exist to prevent widespread internet outages or delays. If one subsea or land cable is damaged, enough alternative links exist to reroute bandwidth and ensure continued coverage.[23] A total internet blackout scenario is far-fetched for most, if not all, Europeans. War games conducted by the Center for a New American Security in 2021 found that Russia would be unable to quickly cut the many cable links between NATO allies in Europe and North America.[24] Nevertheless, European island countries such as Cyprus, Ireland, or Malta, or islands off the coast of the European mainland, are more vulnerable to attacks against their limited number of subsea cables. Below the threshold of a complete outage, adversaries can use cable sabotage—causing delays or temporary loss in connectivity—as a low-cost way of unnerving societies by undermining their sense of security and preparing the ground for a broader attack. And even a modest disruption in internet connectivity that would be a minor nuisance to the general public could have drastic consequences for European and global financial markets, which rely on rapid information flows to optimally perform.[25]

Finally, repair capabilities within Europe are limited.[26] What is more, the depots from which repair vessels operate are vulnerable to attacks. In the event of a coordinated strike against both cables and repair vessels, the resulting damage could be extensive and enduring. This challenge is especially true for cables that run through particularly challenging terrain. For instance, despite warming waters, one key challenge that remains vis-à-vis the construction and repair of future Arctic cable systems is the lack of cable ships with icebreaking capabilities. Currently, no Western cable-laying or repair ships can operate autonomously in areas with heavy sea ice.[27]

In 2021, the U.S. government entered into an agreement with SubCom to establish the Cable Security Fleet, whereby the United States has continuous access to two SubCom cable repair vessels in case of a national emergency for $10 million annually ($5 million per ship).[28] But if a conflict were to break out that involves both the United States and Europe, it is unlikely that two U.S.-flagged vessels would have either the capacity or the mandate to lay, service, and repair any cables of strategic importance in Europe's immediate vicinity—regardless of NATO Article 5 commitments.

An Evolving European Debate on Cable Security and Sovereignty

Recent developments, including damage to subsea cables in the waters near Estonia, Finland, Germany, Norway, and Sweden, have forced Europeans to pay attention to the risk of state and nonstate actors being able and willing to sabotage European underwater infrastructure. The remote nature of most undersea infrastructure and the lack of proper surveillance tools make attribution a challenging task.[29] In the case of undersea infrastructure protection, deterrence is closely intertwined with resilience, as European militaries can only patrol so much area at a given time. To further complicate the picture, civilians can easily be deployed to damage cables in shallower waters near coastlines, blurring the lines between state and nonstate action.

In addition, existing international legal regimes do not adequately protect subsea data cables from intentional damage, nor do they effectively hold perpetrators of such damage accountable.[30] The 1884 Convention for the Protection of Submarine Telegraph Cables (hereafter referred to as the "1884 Cable Convention")—of which several European countries are party to—labels willful or culpably negligent damage to subsea cables a punishable offense.[31] Under Article 21 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS), signatories are also allowed, but not obligated, to adopt necessary laws and regulations to protect subsea cables within their territorial waters.[32] Yet few states in Europe and around the world possess sufficient domestic laws and regulation to specifically protect cables against sabotage within their territorial waters.[33]

Article 113 of UNCLOS also requires signatories to adopt legal instruments to punish ships flying under their flag that are engaged in the willful or culpably negligent damage of subsea cables in areas outside of coastal state sovereignty (more than twelve miles from a nation's seabed).[34] However, there are at least two issues with this provision. First, several UNCLOS signatories have simply not implemented their duties under Article 113. If they have, they are often simultaneously carrying out their 1884 Cable Convention obligations, meaning the measures and associated penalties are outdated and, as one scholar notes, "woefully inadequate."[35] Second, the jurisdiction under Article 113 applies solely to authorities of a country whose flag a ship is flying under—not the countries connected to a particular cable and thereby most directly impacted by any damages. While well-intentioned, the current provisions under international law aimed at protecting subsea cables are not suited for an era of hybrid aggression. But amending UNCLOS to either extend jurisdiction beyond flag states for intentional cable damage on the high seas or require parties to penalize cable sabotage in their territorial waters is unlikely to happen; the amendment process is onerous and has not been attempted. A more likely alternative would be the introduction of a separate treaty instrument for cable protection and security. Perhaps it could be established under UNCLOS, like the recently adopted High Seas Treaty.[36] The EU, as a body inherently focused on the resilience and significance of international legal regimes, could lead the push for such a new instrument.

The context of the war in Ukraine has naturally led European governments and militaries to initially focus on the threat from Russia against their undersea infrastructure. But warnings from the United States, the increasingly blatant Chinese involvement in Russia's war, and recent Chinese involvement in cable-cutting incidents in the Baltic Sea have led Europeans to include China in their risk assessments of undersea cables. Meanwhile, as U.S.-based hyperscalers are disrupting the undersea cable market, some Europeans worry about the competitiveness of European firms and the future of European sovereignty over undersea cables.

Russia: An Acute Threat

Russia has carried out underwater military exercises at depths of more than 6,000 meters. Its attention to transatlantic subsea cables has increased in recent years. In 2023, NATO stated that Russia was "actively mapping" the critical subsea infrastructure of Ukraine's allies.[37] NATO commanders also went on record in April 2023 confirming that they had observed an increase of suspicious Russian activity over and around undersea cables in the Baltic Sea.[38]

These claims have been corroborated by various incidents involving Russian actors in the vicinity of European critical underwater infrastructure. In spring 2023, four Russian commercial and military vessels were monitored sailing through Ireland's Exclusive Economic Zone, rousing suspicion that they could be mapping or interfering with subsea cables off the Irish west coast. Such cables transfer data between the United States and Ireland.[39] More recently, in November 2024, the Irish navy escorted the Russian *Yantar* research vessel out of Irish-controlled waters after it was found patrolling an area where subsea data cables and energy pipelines connect Ireland with Great Britain.[40] Closer to Norway, crew on a Russian vessel that is believed to have been involved in prior damages to subsea cables were caught steering a motorboat near a military garrison in restricted Norwegian waters.[41] These examples have led U.S. officials to the conclusion that "Russia's decision calculus for damaging U.S. and allied undersea critical infrastructure may be changing."[42]

Russia could carry out attacks against undersea infrastructure via its Directorate of Deep-Sea Research, also known as GUGI, which maintains a fleet of quasi-military ships and submarines.[43] Russia's *Yantar* intelligence ship, the same vessel recently escorted out of Irish waters, is equipped with unmanned submarines that could destroy undersea cable infrastructure.[44] Russia is known to use ostensibly civilian scientific research ships to map the Baltic seabed, and such vessels could become involved in cable tampering or sabotage.[45]

Europe has recently experienced several such murky cases. On January 7, 2022, an undersea fiber optic cable connecting the Norwegian archipelago Svalbard to the mainland was severed. Although Russian trawlers were known to be sailing near the damaged cable at the time of the break, there has been no conclusive findings as to what—or who—ultimately caused the damage.[46] Another cable connected to Norway's Evenes Air Station was cut in April 2024. Similar to the Svalbard incident, no suspects have been identified, but Norwegian authorities have declared the damage to be "intentional and calculated."[47]

In November 2024, two cables in the Baltic Sea were severed. The first cable, C-Lion1, which connects data centers in Finland and Germany, is Finland's only undersea data cable to run from the Nordic country directly to central Europe.[48] A second cable connecting Sweden's Gotland Island and Lithuania was also damaged. Authorities suspect the cables to have been damaged by a Chinese-flagged cargo ship, the *Yi Peng 3*, but European lawmakers

and intelligence officials have also hinted at Russian involvement.[49] In a joint statement, the foreign ministers of Germany and Finland wrote, "Our European security is not only under threat from Russia's war of aggression against Ukraine, but also from hybrid warfare by malicious actors."[50] One day after that statement was released, German Defense Minister Boris Pistorius told reporters, "No one believes these cables were cut accidentally."[51] Taken together, NATO defense planners are beginning to consider these incidents a test that demonstrates NATO's potential wartime vulnerabilities.[52]

China: A Newer Risk

In 2020, the U.S. Senate expressed concern to European partners regarding the construction of the Pakistan and East Africa Connecting Europe (PEACE) Cable, a 25,000-kilometer project that connects Singapore to Marseilles, France, with many landing points in South Asia, Africa, and the Middle East in between.[53] PEACE, which went online in March 2022, was installed by HMN Tech, China's leading cable installer (formerly owned by Huawei Technologies).[54] The United States has long advocated against the usage of Chinese components in telecommunications systems, from 5G infrastructure to subsea cables, both domestically and in partner and allied countries.[55]

While Europeans did not share the same risk assessment as the United States in 2020 regarding Chinese involvement in telecommunications equipment, there is much closer alignment today, especially at the EU level.[56] Under von der Leyen, Europe has begun to broadly reevaluate Chinese access to and influence over European critical infrastructure, such as ports, emerging technologies, critical minerals and metals, and telecommunications systems—including undersea cables.[57] In January 2024, the European Parliament also passed a resolution on the security implications of Chinese influence on EU critical infrastructure, in which the body expressed "grave concern over the undersea data cable systems operated by Chinese company HMN Technologies."[58] The resolution labelled HMN Tech a "PLA [People's Liberation Army] cyber intelligence–affiliated entity" and gave particular emphasis to the cybersecurity vulnerabilities associated with cables installed and operated by the Chinese company, including data collection, gathering of intelligence, and underwater surveillance. Since the installation of the PEACE Cable, no subsea cables connecting to Europe have been installed by HMN Tech.

In early October 2023, undersea cables running between Estonia and Finland and Estonia and Sweden were damaged, along with the Balticconnector gas pipeline. The perpetrator was quickly thought to be the *Newnew Polar Bear*, a Hong Kong–flagged, Chinese registered vessel that travelled over all three damage sites at the time of the incidents.[59] The Chinese government later admitted the vessel was responsible for damaging the pipeline and cables, but called the incidents accidents.[60] Finnish and Estonian officials are conducting their own respective investigations into the incident, though have yet to release their findings.[61] During

a visit to Beijing in November 2024, a senior diplomat from Estonia noted that Estonian authorities are still waiting on their Chinese counterparts to "complete the procedures concerning Newnew Polar Bear and its crew, so that we can end the investigation." [62]

One key difference between the 2023 and 2024 Baltic Sea cable cuts is the fate of the suspected vessel immediately following the cable damage. In October 2023, the *Newnew Polar Bear* continued sailing after having damaged two subsea data cables and the Balticconnector pipeline in the Baltic Sea, ultimately returning to port in Tianjin, China. Estonian and Finnish authorities attempted to contact the Hong Kong–flagged vessel but could not forcibly stop or detain the ship without flag state–consent.[63] By comparison, the *Yi Peng 3* has remained at rest in the Kattegat strait, with naval and coast guard vessels from Denmark, Germany, and Sweden in close proximity. Both Danish and Swedish authorities have confirmed that their vessels are present near the *Yi Peng 3*, although they have not revealed whether the ship is officially detained or has been boarded by authorities.[64]

Article 10 of the 1884 Cable Convention allows military vessels under signatories' flags to demand the captain of a nonmilitary vessel, suspected of intentionally damaging subsea cables, to provide evidence of the vessel's nationality.[65] Denmark is a signatory to the 1884 Cable Convention, while Estonia and Finland are not. In its nearly century-and-a-half history, Article 10 has only publicly been invoked once, when crew of the USS *Roy O. Hale* boarded a Soviet trawler believed to have damaged several transatlantic subsea data cables.[66] But if instances of damage and sabotage to undersea infrastructure continue to rise, it is possible that countries will be more willing to use this clause as part of their toolkit in response.

The ongoing inner-European reevaluation of the risks emanating from China has been accompanied by transatlantic policy discussions through the U.S.-EU Trade and Technology Council (TTC), established in June 2021. At the council's first meeting in September of that year, one of the ten TTC working groups was dedicated to "ensuring security, diversity, interoperability, and resilience across the ICT [information and communication technology] supply chain, including . . . undersea cables."[67] In subsequent meetings in 2022 and 2023, this working group discussed the development of alternate cable routes connecting Asia, Europe, and North America, as well as supplier diversification.[68] At least the United States, however, was not satisfied with the outcome of these discussions. In a recent review on U.S.-Europe cooperation on China, the Senate Foreign Affairs Committee assessed that the TTC has delivered no concrete results on subsea cables.[69]

Most recently, the EU—along with Finland, France, the Netherlands, Portugal, and the United Kingdom—endorsed a U.S.-led joint statement in September 2024 on undersea cable security and resilience, emphasizing the importance of "secure and verifiable subsea cable providers for new cable projects."[70] In the document, officially titled The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World, the signatories agree to nine nonbinding principles aimed at improving cable

protection, resiliency, and redundancy. While China is not mentioned explicitly in the text, the principles are clearly directed at Beijing and against the rapid rollout of China's subsea cable industry.[71] In November 2024, only one day after two undersea cables were cut in the Baltic Sea, Norway announced its endorsement of the joint statement.[72]

Although there has been a transatlantic convergence on China with regard to critical infrastructure, EU member states continue to differ with the United States, with each other, and with the European Commission on assessing various risks related to China.[73] European countries vary in their economic dependencies vis-à-vis China and are keen to preserve an independent, national assessment of economic and security vulnerabilities, rather than delegate this responsibility to Brussels.[74] Nevertheless, the Balticconnector incident and the November 2024 cable cuts in the Baltic Sea have opened eyes across Europe to the physical and cybersecurity threat that China could pose to undersea cables connected to the continent. Europeans are also aware that the incoming U.S. administration will likely be less willing to support Ukraine if they perceive Europe as being lenient toward China—contributing another factor to the debate in Europe on security threats posed by Beijing.

United States: A Partner and Competitor

The United States and European governments have been engaged in close discussions on subsea cables, including through the TTC. But close collaboration is complicated by the fact that companies on both sides of the Atlantic also are direct competitors. For example, an EU-backed Arctic cable initiative was withdrawn as part of the TTC agreement after a U.S.-supported cable constructed by a different company took a similar route.[75] Moreover, European actors are concerned with the emerging dominance of a select few U.S. companies in new cable investment and construction. These hyperscalers, namely Amazon, Google, Meta, and Microsoft, accounted for nearly a quarter of cable systems that began operation between 2019 and 2023 and have flipped the traditional subsea cable investment model on its head.[76] While Europe is home to ASN, the global market leader in subsea cable installation, it lacks a peer competitor to the hyperscalers that are shaping the future of cable investment. Initiatives such as Gaia-X, conceived to create a European cloud platform able to compete with the U.S. hyperscalers, have failed to get off the ground.[77] As U.S. hyperscalers continue to occupy a larger market share, the chances rise that they push out European telecommunications firms, or other traditional investors in cables, in the process.

Certain observers in Europe, and especially in France, have taken issue with this consolidation in the submarine cable market, arguing that a small number of U.S. tech companies now possess "unlimited power over the sector."[78] Others have taken a more resigned approach, including former Italian prime minister Mario Draghi, who recently wrote in his report on European economic competitiveness that "it is too late for the EU to try and develop systematic challengers to the major U.S. cloud providers."[79] In the context of subsea

cables, Europeans are aware of their dependencies on both U.S. firms and Chinese firms, particularly when it comes to main investors in cables, but are unable to easily rid themselves of these dependencies.

Any comparison of global competitiveness in the field of subsea cables must look at all levels of the subsea cable supply and investment chain. Table 1 shows the relative dominance of Chinese, U.S., European, and Japanese companies in different links of the chain. Even though China's HMN Tech has emerged in the international subsea cable supplier market at an impressive pace, its total market share is still quite small compared to ASN and SubCom. From 2020 to 2024, ASN and SubCom supplied approximately 34 percent and 19 percent of new subsea cable systems built, respectively, while HMN Tech was responsible for 10 percent.[80] Efforts led by the United States to limit the reach of subsea cables built by Chinese suppliers also appear to be working. Whereas HMN Tech provided an estimated 10 percent of new kilometers of subsea cables entering service between 2010 and 2023, that number is only 4 percent for systems planned through 2026.[81]

Table 1. Key National Players in Subsea Cable Supply and Investment Chains

	Chinese companies	U.S. companies	European companies	Japanese companies
Main investors	China Telecom China Mobile China Unicom	Google Amazon Meta	n/a	n/a
Cable builders	HMN Tech FiberHome	SubCom	ASN (France)	NEC
Fiber optic cables	Hengtong FiberHome Yangtze Optical Fibre and Cable Jiangsu Zhongtian Technology	Corning	Nexans (France)	NEC Furukawa Electric
Optical components, chips	Wuhan Fisilink Microelectronics Technology Huawei Technologies Zhongji InnoLight Accelink Technologies	Broadcom Coherent	n/a	Sumitomo Electric Industries
Repeaters	HMN Tech FiberHome	SubCom	n/a	NEC
Cable ship operators	FiberHome Marine China Submarine Cable Construction S.B. Submarine Systems	SubCom	Orange (France) Global Marine Group (UK) ASN (France)	NTT WE Marine
Data center, server makers	Huawei Inspur Lenovo	Google Amazon Meta	n/a	n/a

Source: Cheng Ting-Fang, Lauly Li, Tsubasa Suruga, and Shunsuke Tabeta, "China's Undersea Cable Drive Defies U.S. Sanctions," *Nikkei Asia*, June 26, 2024, https://asia.nikkei.com/Spotlight/The-Big-Story/China-s-undersea-cable-drive-defies-U.S.-sanctions. Submarine Telecoms Forum, "Industry Report, 2024–2025: Issue 13."

As Europeans recognize the geopolitical importance of undersea cables, they might consider ways to ensure that ASN remains globally competitive, especially as the United States and China are investing in their own national champions. American policymakers, too, should want the companies of their close allies in Europe to remain viable market players. EU state aid regulations generally prohibit an individual company from receiving government support "unless exceptionally justified."[82] However, with the reelection of von der Leyen as European Commission president, it appears that attitudes toward state aid, particularly in strategically significant domains, might be shifting. Indeed, von der Leyen has instructed newly appointed European Executive Vice President for Clean, Just, and Competitive Transition Teresa Ribera to "modernise the EU's competition policy to ensure it supports European companies to innovate, compete and lead world-wide."[83]

Emerging European Responses

NATO, the EU, and certain European governments have all increased their efforts to better protect existing subsea cable infrastructure in a heightened threat environment. Effectively protecting subsea cables against all forms of attack and sabotage would ideally require surface and undersea surveillance along the entire length of the cables. But beyond the technical difficulties of such an approach, undersea cables cross territorial waters, exclusive economic zones, and the high seas, further complicating total surveillance from a regulatory perspective. One significant challenge is coordination: private operators, policymakers, militaries, police, and coast guards all share some responsibility for securing undersea cables, but the distribution of this responsibility varies from country to country.[84] Even close to their own shores, governments struggle to acquire a fully integrated operational picture of activity below and above water.[85]

Securing, Protecting, and Repairing Europe's Cables

As Europe's leading military alliance, NATO has long been aware of vulnerabilities to member states' critical undersea infrastructure but has only recently placed focus on protection strategies, including subsea surveillance.[86] The alliance has ramped up its air and naval patrols and exercises in the North and Baltic Sea, where Russian ships are increasing their own activities.[87] NATO has also tasked its Joint Force Command Norfolk with undersea threat monitoring and subsea infrastructure protection; and, at its summit in Vilnius, Lithuania, in July 2023, NATO established a Maritime Centre for the Security of Critical Undersea Infrastructure in the United Kingdom.[88] In October 2023, NATO defense ministers endorsed a new Digital Ocean Vision, an initiative aimed at enhancing maritime situational awareness and surveillance "from seabed to space."[89] The alliance has incorporated the initiative in recent joint exercises, testing maritime unmanned systems during

the Dynamic Messenger 23 exercise in September 2023 and the REPMUS 24 exercise in September 2024.[90] And in November 2024, Polish Prime Minister Donald Tusk proposed a new Baltic Sea maritime patrol program.[91]

Some larger European countries are exploring ways to improve their own undersea surveillance capabilities. Since releasing a Seabed Warfare Strategy in February 2022, France has invested in the development of undersea drones and surveillance infrastructure.[92] In October 2024, the French Navy ordered an autonomous underwater vehicle capable of operating as deep as 6,000 meters below the surface.[93] Italy has similarly increased its undersea surveillance capacities following the Nord Stream explosions.[94] In 2021, the United Kingdom announced the launch of two multirole surveillance ships, designed to support various underwater operations, including undersea surveillance and cable protection.[95] The first of the two ships, the *RFA Proteus*, formally entered service in October 2023.[96]

Regarding the cybersecurity of Europe's subsea data cables, at a meeting in Nevers, France, in March 2022, EU telecommunications ministers released a statement, the Nevers Call to Reinforce the EU's Cybersecurity Capabilities (hereafter referred to as the Nevers Call), in which they labelled telecommunications networks as "prime target[s]" for cyber attacks.[97] Shortly after the release of the Nevers Call, in December 2022, the EU adopted a new directive on cybersecurity, known as the NIS2 Directive, urging member states to, among other actions, include the cybersecurity of undersea communications cables in their national security strategies, map for potential cybersecurity risks, and deploy mitigation measures.[98] In its June 2023 Final Assessment Report, the EU-NATO Task Force on the Resilience of Critical Infrastructure recommended the promotion of best practice exchanges between civilian and military actors on implementing relevant cyber-related policies and legislation.[99] In February 2024, the European Commission released its first Recommendation on Secure and Resilient Submarine Cable Infrastructures, which included the need for more frequent risk assessments and stress tests on the cybersecurity and physical security of subsea cable systems.[100] The 2024 recommendation also calls for enhanced information sharing between member states and better cable maintenance and repair capabilities. Finally, the 2024 New York Joint Statement, of which the EU is a signed party, calls for signatories to build and maintain their subsea cable infrastructure, "incorporating cybersecurity best practices that safely facilitate international communication."[101] But the effectiveness of these measures depends on national capitals' willingness to cooperate and to effectively and quickly implement them.

To sustainably ensure the physical and cybersecurity of their undersea infrastructure, Europeans must acquire a clearer picture of their assets and vulnerabilities. To that end, the European Commission wants to map and review the subsea cables connecting Europe to identify potential weak spots. EU officials are concerned that they do not possess a clear sense of who owns and operates European undersea infrastructure.[102] They want a more centralized overview of private sector data in order to identify potential issues related to high-risk owners and guarantee that there is enough diversity and redundancy in Europe's

undersea infrastructure network to ensure the security of data supply. The United States has created a similar dedicated review process, intent on restricting the use of equipment by untrustworthy suppliers in cable systems.[103]

EU policymakers face several obstacles. First, it is difficult to convince member states to share information. As an institution, the European Commission is relatively new to European security and defense and has little practice with managing sensitive information. EU member states are reluctant to share details about their critical infrastructure with each other, let alone a third party such as the commission.[104] As a result, the commission has so far had to work mostly with public data about Europe's subsea cables. The second challenge faced by all European policymakers is accessing and integrating data from the different private companies that operate subsea cables connected to Europe. In Europe, 80 percent of all critical infrastructure is owned or controlled by private entities, which means that it is the civilian industry that has the capacity to survey undersea cables and map vulnerabilities.[105] This dynamic requires a concerted focus on building robust public-private partnerships.

With this in mind, in February 2023, NATO stood up a new Critical Undersea Infrastructure Coordination Cell in Brussels to operate as a strategic hub between NATO allies, partners, and the private sector, which held its first meeting in May 2024.[106] The cell convenes military and civilian officials, as well as business representatives, to map vulnerabilities and synchronize efforts between governments and the private sector. NATO-EU cooperation on subsea cable protection is critical and an obvious step: protecting critical infrastructure from threats requires an approach that merges both military and civilian measures. To this end, the two organizations have created an EU-NATO Task Force on critical infrastructure resilience.[107]

Complementary to efforts taken at the NATO and EU levels, various constellations of European countries have also emerged to protect subsea cables against physical attacks and sabotage. The Joint Expeditionary Force (JEF), made up of the United Kingdom, the five Nordic countries, the three Baltics, and the Netherlands, agreed in June 2023 to accelerate cooperation to "detect, deter, and respond to threats against our critical undersea and offshore infrastructure."[108] Months later, in December 2023, the JEF conducted a joint exercise in the Baltic Sea focused on subsea infrastructure protection.[109]

Additionally, in April 2024, six North Sea countries (Belgium, Denmark, Germany, the Netherlands, Norway, and the United Kingdom) pledged to improve information and knowledge sharing to better protect critical undersea infrastructure from foreign interference and disruption.[110] Individual European governments have also taken steps to strengthen public-private partnerships regarding undersea cables. For instance, after the Balticconnector pipeline incident last fall, the Norwegian government cooperated with its energy companies to first map oil and gas pipelines and then the electrical grid and subsea cables.[111]

The EU and NATO can also help to incentivize the development of new technologies needed to secure and protect current and future subsea cables. For instance, EU member

states Greece, Italy, Poland, and Portugal have joined forces under the union's defense framework, Permanent Structured Cooperation or PESCO, to work on the Harbour & Maritime Surveillance and Protection project.[112] The aim is to develop integrated systems of maritime sensors, software, and platforms, which will fuse and process data to detect and identify potential maritime threats. Belgium, France, Germany, Ireland, Italy, Portugal, Spain, and Sweden are also working on a project, which aims to increase the EU's operational efficiency in the protection of critical maritime infrastructure protection.[113] NATO is similarly investing in resilience by funding research into ways to seamlessly reroute internet traffic from subsea cables to satellites in the event of natural disasters or sabotage.[114]

Competing for Global Influence

China is investing in subsea cable projects around the world not only to boost connectivity and increase redundancies in its immediate surroundings but also to deepen its geopolitical influence in strategic regions. As part of its broader Belt and Road Initiative (BRI), the Chinese government in 2015 announced its plans for a Digital Silk Road Initiative (DSRI), through which Beijing would invest vast sums of money in developing countries' digital infrastructure.[115] Although not explicitly part of these investment deals, the Chinese government has expected and often received political and diplomatic sway in return among recipient countries.[116] Both the United States and the EU have each launched similar mechanisms aimed at countering Chinese influence in developing countries and regions, yet these programs fail to match the BRI or DSRI in scale.[117]

The EU's Global Gateway initiative was launched in 2021 as an alternative offer to countries considering Chinese strategic funding of physical and digital infrastructure through BRI and DSRI. Through this €300 billion (nearly $318 billion) instrument, the EU wants to establish strategic links with developing regions—especially Africa—and avoid overreliance on geographical chokepoints, such as critical minerals sourced from China.[118] The EU funds digital infrastructure projects under the auspices of Global Gateway, through the Connecting Europe Facility (CEF). CEF Digital was initially allocated a budget of €1.6 billion ($1.7 billion) for 2021–2027, with €389 million ($412 million) of that sum earmarked for "backbone connectivity projects," of which the vast majority of funding has gone toward the construction of subsea cables either between EU countries or between member states and third countries.[119] In its most recent CEF Digital call for proposals, the European Commission wrote that "CEF Digital is expected to be one of the main funding instruments for secure and resilient submarine cables reinforcing the links between Member States."[120]

Nearly halfway into the 2021–2027 funding period, Brussels has already spent or committed more than the initial €389 million set aside for these backbone connectivity projects through CEF Digital. Since 2022, after three rounds of proposals, forty-six subsea cable works and studies projects have been awarded at least partial funding under CEF Digital for a total of approximately €412 million ($436 million). The EU recently announced an additional €542 million (nearly $574 million) for backbone connectivity projects through CEF Digital for

the 2024–2027 period.[121] If this amount is spent in its entirety, the EU will have invested nearly €1 billion on subsea data cable projects from 2021–2027. To be sure, the amount is a drop in the bucket compared to the financial commitments made by China under its DSRI. Nevertheless, the projected increase in funding dedicated to subsea cable projects by the European Commission signifies the issue being taken more seriously in Brussels.

Despite this financial commitment, several factors indicate that this money is either not adequate or not being allocated in a strategic manner. The European Commission wishes to spread the money it spends on subsea cables across multiple projects, rather than fewer, costlier projects.[122] This approach has led to a mismatch in financing for the projects the European Commission deemed to be most important and the total funding that these projects receive. In doing so, the commission risks partially funding projects of great geopolitical significance that do not receive enough private financing to be completed.

To address this problem, the commission has tasked a group of experts to identify strategic Cable Projects of European Interest (CPEIs) that the EU should invest in. This group will assist an evaluation committee in assessing EU-funded projects based on five criteria: priority and urgency, maturity, catalytic effect, impact, and quality.[123] Yet it remains unclear how much weight the experts' feedback on CPEIs has on any decisions regarding CEF Digital funding compared to national and distributional interests. Each approved project must receive a score of three out of five or higher for each of the five criteria, and EU officials have labelled previous CEF Digital funding allocations as political decisions lacking in transparency.[124] Moreover, the projects that receive the highest score from the evaluation committee rarely receive their full grant requests, compared to lower-ranking applications.[125]

The geographical distribution of subsea cable projects that have received EU funding thus far also raises questions about the EU's strategic approach in expanding its undersea digital network. EU CEF subsea cable projects have largely focused on boosting redundancies in and around Europe and its outermost regions. Much fewer projects connect the EU to third countries, including African countries (especially beyond Tunisia or Morocco) and Latin American countries (beyond extending the pre-existing EllaLink cable, which connects Brazil to Portugal).

Three strategically important regions that the EU has begun to focus on regarding new subsea cables are the Arctic, the Black Sea, and South Asia, particularly India.

Regarding the Artic region, as warmer global temperatures melt ice in the Arctic Ocean, new digital connection routes are emerging. Not only would a cable laid through the Arctic that connects, for example, Europe to Asia be much shorter than existing infrastructure, reducing transmission time, but it would also avoid current chokepoints or flashpoints such as the Suez Canal and the Red Sea.[126] Moreover, the remaining ice cover grants natural protection against human tampering with cables for much of the year. The EU has already allocated some funding to separate Arctic cable projects, including the Far North Fiber

and the Polar Connect cables.[127] But more can be done to see these projects to completion, including support for cable ships with icebreaking capabilities and more adequate funding for grant requests in future CEF Digital calls.

In the Black Sea, the EU intends on investing in a new undersea data cable that would connect EU member states with Georgia.[128] Not only would this cable improve Georgia's digital connectivity, but it would also reduce the country's dependence on cables running through Russia. In addition to this planned cable, which is still in the feasibility assessment stage, the EU has invested a small amount of money (€57,500, or around $61,000) through CEF Digital to investigate possible subsea cable landing points along Bulgaria's Black Sea coast. Such projects are crucial in the context of protecting EU accession countries against an emboldened Russia, although it remains unclear how fast cables can currently be laid in the Black Sea with Russia's ongoing military activity there.

Finally, the India-Middle East-Europe Economic Corridor (IMEC), announced at the September 2023 G20 Summit, includes plans for boosting connectivity between Europe and India through subsea cables, such as the Blue and Raman cable systems.[129] Blue-Raman, which is currently under construction, will connect Europe to India while bypassing Egypt—cementing the Gulf's role as a "digital anchor" between Europe and India.[130] Google and ASN are the primary investors and cable suppliers in the Blue-Raman cable systems, introducing a potential challenge to Huawei's digital dominance in the Gulf to date. European, Middle Eastern, and Indian participants of the IMEC will have to negotiate these tensions.

Recommendations

Europeans are beginning to act to better protect and expand upon their existing undersea cable systems. Below are a series of recommendations that identify gaps in current European strategies vis-à-vis undersea cables and provide steps to address existing shortcomings. Directed at European lawmakers, these recommendations aim to ensure that European countries maintain their edge in subsea cable installation; are better prepared to protect and repair damaged cable systems; and strategically leverage global partnerships across cables' lifespan, from component sourcing, to route planning and installation, and finally to maintenance and repair.

Map vulnerabilities. In spite of the flurry of recent initiatives to protect and secure European subsea cables, the level of understanding and preparedness still varies from country to country. The challenge is to ensure the same level of security across European borders. The EU's regulatory power is one useful tool to promote the uniform application of high security standards. Gathering a more complete picture of Europe's undersea infrastructure

is crucial. To this end, the EU and NATO must invest in the exchange of know-how and technologies between allied governments and between public and private actors, and earn the trust of all relevant stakeholders to pursue collective solutions.

Invest in secure supply chains. Europeans should invest in secure supply chains for the components of subsea data cables, including metals such as steel and copper, silicon, and fiber optic components. These efforts should be done in partnership with like-minded countries, including, for instance, signatories of the New York Joint Statement. The signatories should also commit to increase information sharing about the sources of components and cable services. Such information exchanges should take place for all life stages of the cables, including during deployment, maintenance, and repair. Where possible, efforts by European actors to secure the subsea cable supply chain with strategic partners can work hand in hand with secure supply chain initiatives around the clean energy transition, such as those discussed as part of the U.S.-EU TTC.[131]

Invest in infrastructure protection technology. The EU should use its defense industrial research and development funding tools, such as the European Defense Fund, to support member-state investment in technologies to protect undersea cables and landing stations. It could, for instance, fund research on better sensor technology to map the seafloor and enable the long-term monitoring of underwater infrastructure and to deter attacks or at least detect damage more easily. Any new EU-funded cables should be built with those features. The EU might also consider including a dedicated envelope in the EU budget to allow governments to invest in protecting their critical infrastructure.[132] There is opportunity to partner with the United States, here, too—through NATO's defense innovation funding tools, for instance.

Stand up joint naval policing missions. In response to the November 2024 undersea cable cuts in the Baltic Sea, Polish Prime Minister Tusk urged his Baltic and Nordic counterparts to establish a joint naval policing mission to better protect their undersea infrastructure against external security threats. The program would operate in parallel to the preexisting joint Baltic Air Policing mission.[133] Baltic Sea region states should implement this proposal as quickly as possible and should share best practices with other NATO allies. Indeed, if this initiative is successful in the Baltic Sea, similar regional initiatives within NATO could be created to boost deterrence against threats to undersea infrastructure in the North Sea, the Mediterranean, and the North Atlantic.

Reduce cybersecurity risks and vulnerabilities. European actors are aware that subsea data cables are susceptible to cyber as well as physical attacks and have on multiple occasions called on EU and NATO member states to mitigate cybersecurity risks in their subsea cable systems and exchange best practices with one another. EU member states should implement recommendations under the NIS2 Directive, with respect to both subsea data cables and cable landing stations. EU and NATO officials should also ensure that subsea cable systems are a standing agenda item for discussion in Structured Dialogues on Cyber—the first of which was held in October 2024.[134] Through its Critical Undersea Infrastructure Coordination Cell in Brussels, NATO should facilitate and deepen exchanges with private

sector actors involved in cable installation and repair, as well as in network management and data security.

Strengthen legal instruments for cable protection. All EU countries, and nearly all European NATO members (absent Türkiye), that are connected to subsea data cables have ratified UNCLOS. The same is not true of the 1884 Cable Convention. Bulgaria, Croatia, Cyprus, Estonia, Finland, Ireland, Latvia, and Lithuania all have yet to ratify the treaty and should do so immediately. It is currently only the 1884 Cable Convention—and not UNCLOS—that grants military vessels the power to stop nonmilitary ships suspected of damaging subsea cables.[135] All European countries should also review their respective criminal codes related to Article 21 of UNCLOS—which grants states permission to penalize willful damage to subsea cables in their territorial waters—to ensure they possess specific penal consequences for sabotage against subsea cables and that such consequences are of an adequate degree. These measures should be coordinated among EU and NATO members to ensure legal standardization in all European waters. Finally, EU governments should explore avenues to begin negotiations on a new treaty instrument, under UNCLOS, that addresses the current international legal shortcomings regarding cable protection and security.

Invest in cable repair capabilities. The EU should provide funding to create its own version of the U.S. Cable Security Fleet. Alternatively, as suggested in a 2024 U.S. Senate Foreign Relations Committee report, the United States could expand its Cable Security Fleet to "work with European partners."[136] Europeans should also work with, and offer support to, smaller partner countries who lack access to repair capacities. And they should do more to bolster their subsea cable-laying and repair capabilities for future geographically challenging cable routes, including in the Arctic. Whether retrofitting existing icebreakers with cable-laying capabilities or constructing new vessels entirely, Europe has an opportunity to take the lead in the emerging domain of subsea Arctic cable laying and repair.

Avoid bureaucracy. The EU and NATO have important resources and regulatory and budgetary tools to support Europeans in their efforts to secure and protect their undersea infrastructure. But they should learn from their ally: in the United States, a centralized approach has led to complaints about bureaucratic delays in the process of licensing subsea cables and vetting the trustworthiness of suppliers, significantly slowing down the process for all involved stakeholders.[137] Brussels institutions becoming more involved in the issue must avoid setting up excessive bureaucratic and opaque processes. They can do so by ensuring robust dialogue takes place between European security, regulation, and industry communities in settings such as NATO's Coordination Cell.

Invest in Europe's strengths. Possessing the current market leader in subsea cable installation should not encourage complacency in Europe. Drastic increases—as well as more strategic thinking—in resource allocation are still necessary if the EU wishes to compete with both China and the United States in future cable projects. Although achieving full European digital autonomy is unlikely given the lack of hyperscalers and cloud providers in Europe, there are still ample areas for the EU and individual European countries to increase investment related to subsea cable systems.

Seek out opportunities for allied business collaboration. There will be many instances where European cable companies, such as ASN, are in direct competition with their U.S. and Japanese counterparts, including SubCom and NEC. Yet if the ultimate goal of U.S. and, to a less extreme extent, European strategy vis-à-vis undersea data cables is to restrict the rise and dominance of Chinese players such as HMN Tech, then more emphasis and attention should be given to opportunities for collaboration between U.S., European, and other allied cable construction firms. One concrete agenda item for Europeans to discuss with the incoming U.S. administration would be the establishment of technology sharing or joint venture agreements between U.S. and European cable companies, potentially through the new NATO Critical Undersea Infrastructure Coordination Cell in Brussels.[138]

Reform EU funding for cable projects. Having the EU fund subsea cable projects through CEF Digital is useful. Yet future funding calls should address the mismatch in the geostrategic significance of potential cable projects and EU-allocated money. The European Commission would put its money to better use if it provided more funding for a select number of strategically important projects, rather than continuing to spread its allocated funds wider with every new call for proposals. The EU should also include geopolitical importance as a concrete criterion by which it evaluates CEF Digital applications. Although applicants are encouraged to demonstrate that their proposal has geostrategic importance, potentially funded projects are not currently evaluated on this merit.[139]

Improve cable governance. Several entities are responsible at the national, EU, and international levels for the regulation and protection of subsea cables. For example, national telecom authorities often supervise the security of public communication networks while navies, coast guards, and police forces oversee the protection of physical infrastructure.[140] EU member states should stand up interagency working groups dedicated specifically to subsea cable regulation and security. Each EU member state should also have a specific point of contact regarding its subsea cable infrastructure, so as to maximize efficiency and efficacy of inter-European communication on undersea cables. European governments should work to ensure that both European officials and private sector actors are well-represented in international fora related to subsea cable security and resilience.

Expand international cable partnerships. In April 2022, the EU and India launched their own Trade and Technology Council (TTC), Brussels' second such endeavor after its TTC with the United States.[141] Unlike its TTC with Washington, the EU-India TTC does not have a working group that covers subsea data cables. Leaders in Brussels and New Delhi should change this, particularly as digital connections between Europe and India increase as the IMEC progresses. The EU should also leverage its expertise and market advantages in subsea cable construction and repair to provide training assistance to third countries, especially if these countries are being encouraged to either phase out high-risk vendors from their cable systems or opt for U.S. or European alternatives.

About the Authors

Sophia Besch is a senior fellow in the Europe Program at the Carnegie Endowment for International Peace. Her area of expertise is European defense policy.

Erik Brown is a James C. Gaither Junior Fellow in the Europe Program.

Acknowledgments

The authors would like to express their sincere thanks to Katrine Westgaard for her stellar research assistance in an early phase of this project.

Notes

1 Leo Laikola, Kati Pohjanpalo, and Milda Seputyte, "Finland and Lithuania Report Severed Undersea Data Cables," *Bloomberg*, November 18, 2024, https://www.bloomberg.com/news/articles/2024-11-18/finland-says-subsea-germany-link-serving-data-centers-is-severed; and Ivana Kottasova, Billy Stockwell, and Paul P. Murphy, "Two Undersea Cables in Baltic Sea Disrupted, Sparking Warnings of Possible 'Hybrid Warfare,'" CNN, November 18, 2024, https://www.cnn.com/2024/11/18/europe/undersea-cable-disrupted-germany-finland-intl/index.html.

2 Shashank Joshi, "How China and Russia Could Hobble the Internet," *Economist*, July 11, 2024, https://www.economist.com/international/2024/07/11/how-china-and-russia-could-hobble-the-internet; and Olga Khazan, "The Creepy, Long-Standing Practice of Undersea Cable Tapping," *Atlantic*, July 16, 2013, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

3 Justin Sherman, "Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security," Atlantic Council, September 13, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/#recommendations; and Colin Wall and Pierre Morcos, "Invisible and Vital: Undersea Cables and Transatlantic Security," Center for Strategic and International Studies, June 11, 2021, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security.

4 Georgia Bafoutsou, Maria Papaphilippou, and Marnix Dekker, "Subsea Cables—What Is at Stake?," European Union Agency for Cybersecurity, July 2023, 20, https://www.enisa.europa.eu/news/dive-into-the-deep-sea-a-view-of-the-subsea-cable-ecosystem.

5 "Subsea Cables: What is at stake?", ENISA, July 2023, https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf.

6 Jeremy Page, Kate O'Keeffe, and Rob Taylor, "America's Undersea Battle With China for Control of the Global Internet Grid," *Wall Street Journal*, March 12, 2019, https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466?mod=article_inline.

7 Théophane Hartmann, "Submarine Cables: Commission Suggests Phase-out of High-Risk Vendors," Euractiv, February 15, 2024, https://www.euractiv.com/section/digital/news/submarine-cables-commission-suggests-phase-out-of-high-risk-vendors/.

8 Todd Young, Christopher S. Murphy, Marco Rubio, Tim Kaine, Pete Ricketts, et al., "Letter to POTUS on Undersea Cable Security," October 21, 2024, https://www.young.senate.gov/wp-content/uploads/10212024-Letter-to-POTUS-on-Undersea-Cable-Security.pdf.

9 Joe Brock, "U.S. and China Wage War Beneath the Waves—Over Internet Cables," Reuters, March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.
10 Aurélie Pugnet, "NATO promises better strategy against cyber attacks and undersea cables," Euractiv, December 4, 2024, https://www.euractiv.com/section/global-europe/news/nato-promises-better-strategy-against-cyber-attacks-and-undersea-cables/.
11 "Digital Economy and Society Statistics—Households and Individuals," Eurostat, April 2024, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Use_of_internet.
12 Jannik Hartmann, "Protecting the EU's Submarine Cable Infrastructure," German Council on Foreign Relations, July 10, 2023, https://dgap.org/en/research/publications/protecting-eus-submarine-cable-infrastructure#:~:text=About%20250%20active%20cables%20ensure,EU%20member%20states%20and%20allies.
13 Charlie Cooper, "NATO Warns Russia Could Target Undersea Pipelines and Cables," POLITICO, May 3, 2023, https://www.politico.eu/article/nato-warns-russia-could-target-undersea-pipelines-and-cables/.
14 Laura Kabelka, "EU Aims to Tackle Threats to Submarine Data Cables," Euractiv, October 6, 2022, https://www.euractiv.com/section/digital/news/eu-aims-to-tackle-threats-to-submarine-data-cables/.
15 Submarine Telecoms Forum, "Industry Report, 2024–2025: Issue 13," 2023, https://subtelforum.com/industry-report/, 74.
16 Ibid., 75.
17 Daniele Lepido, "Telecom Italia Is Set to Reject Italy's Bid for Subsea Cable Unit," Bloomberg, February 6, 2024, https://www.bloomberg.com/news/articles/2024-02-06/telecom-italia-rejects-italy-government-bid-for-sparkle; and Daniele Lepido, "Italy, Asterion Make New Bid on Telecom Italia Subsea Cable Unit," Bloomberg, October 2, 2024, https://www.bloomberg.com/news/articles/2024-10-02/italy-asterion-make-new-bid-on-telecom-italia-subsea-cable-unit.
18 Olivier Pinaud, "'Strategic' Submarine Telecom Cable Manufacturer ASN Nationalized by France," *Le Monde*, November 5, 2024, https://www.lemonde.fr/en/economy/article/2024/11/05/asn-strategic-manufacturer-of-submarine-telecom-cables-nationalized-by-france_6731573_19.html.
19 Jocelinn Kang and Jessie Jacob, "Connecting the Indo-Pacific: The future of subsea cables and opportunities for Australia," Australian Strategic Policy Institute, September, 25, 2024, 7, https://www.aspi.org.au/report/connecting-indo-pacific-future-subsea-cables-and-opportunities-australia.
20 Olivier Pinaud, "Big Tech Colonizes Seabed to Assert Control of the Internet," *Le Monde*, January 3, 2023, https://www.lemonde.fr/en/international/article/2023/01/02/big-tech-colonizes-seabed-to-assert-control-of-the-internet_6010073_4.html?random=817152304.
21 Submarine Telecoms Forum, "Industry Report, 2024–2025: Issue 13," 94.
22 Josh Dzieza, "The Cloud Under the Sea," The Verge, April 16, 2024, https://www.theverge.com/c/24070570/internet-cables-undersea-deep-repair-ships.
23 The recent cable cuts in the Baltic Sea and the lack of significant internet outages highlight this point. Emile Aben, "Does the Internet Route Around Damage? – Baltic Sea Cable Cuts," RIPE Labs, November 20, 2024, https://labs.ripe.net/author/emileaben/does-the-internet-route-around-damage-baltic-sea-cable-cuts/.
24 Chris Dougherty, "More Than Half the Battle: Information and Command in a New American Way of War," Center for a New American Security, May 2021, 18, https://s3.amazonaws.com/files.cnas.org/CNAS+Report-Command+and+Info-2021.pdf.
25 Virginia Petrou, "Navigating the Underwater Threat: Risks of Subsea Cable Disruptions for Financial Services," BSO, June 1, 2023, https://www.bso.co/all-insights/mitigate-risk-of-subsea-cables-disruptions-finacial-services.
26 Christian Bueger, Tobias Liebetrau, and Jonas Franken, "Security Threats to Undersea Communications Cables and Infrastructure—Consequences for the EU," European Parliament, June 2022, https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf.
27 "The Government Is Investigating Possibilities for New Polar Research Vessel," Swedish Polar Research Secretariat, January 8, 2024, https://www.polar.se/en/news/2024/the-government-is-investigating-possibilities-for-new-polar-research-vessel/#:~:text=via%20the%20Arctic.-,Currently%2C%20no%20Western%20ship%20has%20the,capacity%20needed%20for%20cable%20laying.&text=During%20the%20design%20work%2C%20the,for%20tasks%20within%20total%20defence.
28 "Chapter 532—Cable Security Fleet," https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title46-chapter532&edition=prelim. Interestingly, funding for the Cable Security Fleet was excluded in DOT's FY2025 proposed budget.

29 "Bojan Pancevski, "Europe Sees Signs of Russian Sabotage but Hesitates to Blame Kremlin," *Wall Street Journal*, May 20, 2024, https://www.wsj.com/world/europe/europe-sees-signs-of-russian-sabotage-but-hesitates-to-blame-kremlin-72598d4b?mod=article_inline&mod=article_inline.

30 Robert Beckman, "Protecting Submarine Cables from Intentional Damage—The Security Gap," in *Submarine Cables: The Handbook of Law and Policy*, eds. Douglas R. Burnett, Robert Beckman, and Tara M. Davenport (Leiden: Martinus Nijhoff Publishers, October 2013), 281–297.

31 "Convention for the Protection of Submarine Telegraph Cables," Article 2, opened for signature March 14, 1884, Department of Foreign Affairs and Trade Canberra, https://iscpc.org/information/Convention_on_Protection%20_of_Cables_1884.pdf.

32 "United Nations Convention on the Law of the Sea," Article 21, opened for signature December 10, 1982, United Nations, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

33 Tara Davenport, "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis," *Catholic University Journal of Law and Technology* 24, no. 1 (December 2015): 83, https://scholarship.law.edu/cgi/viewcontent.cgi?article=1001&context=jlt.

34 "United Nations Convention on the Law of the Sea," Article 113.

35 Ibid.

36 Author interview with an expert on international maritime law, November 26, 2024.

37 Cooper, "NATO Warns Russia Could Target Undersea Pipelines and Cables."

38 Jim Sciutto, "US Sees Increasing Risk of Russian 'Sabotage' of Key Undersea Cables by Secretive Military Unit," CNN, September 6, 2024, https://www.cnn.com/2024/09/06/politics/us-sees-increasing-risk-of-russian-sabotage-undersea-cables/index.html.

39 Conor Gallagher, "Defence Forces Monitor Armed Russian Naval Vessel Off West Coast," *The Irish Times*, May 7, 2023, https://www.irishtimes.com/ireland/2023/05/07/defence-forces-monitor-armed-russian-naval-vessel-off-west-coast/.

40 Cormac O'Keeffe, "Navy Vessel Escorts Russian 'Subsea Spy Ship' Out of Irish Water," *Irish Examiner*, November 16, 2024, https://www.irishexaminer.com/news/arid-41517743.html.

41 Ben Taub, "Russia's Espionage War in the Arctic," *New Yorker*, September 9, 2024, https://www.newyorker.com/magazine/2024/09/16/russias-espionage-war-in-the-arctic?_sp=356cd344-ffbd-4127-baec-5ffd923a8c60.1726490061412.

42 Sciutto, "US Sees Increasing Risk of Russian 'Sabotage' of Key Undersea Cables by Secretive Military Unit."

43 Hotaka Nakamura, "Defending Submarine Cables in the Black Sea: A Challenge for NATO and the Region," Middle East Institute, March 2, 2023, https://www.mei.edu/publications/defending-submarine-cables-black-sea-challenge-nato-and-region; and Frank Umbach, "New Challenges in Protecting Critical EU Infrastructure," GIS Reports Online, February 6, 2023, https://www.gisreportsonline.com/r/europe-critical-infrastructure/.

44 Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," Royal United Services Institute, May 25, 2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.

45 Jack Detsch and Keith Johnson, "NATO Wants to Boost Its Undersea Defenses," *Foreign Policy*, June 24, 2024, https://foreignpolicy.com/2024/06/24/nato-undersea-cable-network-russia-infrastructure-defense/.

46 Benjamin Fredriksen, "Kabelmysteriene," NRK, June 26, 2022, https://www.nrk.no/nordland/xl/russiske-tralere-krysset-kabler-i-vesteralen-og-svalbard-for-brudd-1.16007084; and Håvard Gulldahl and Inghild Eriksen, "This Is What the Damaged Svalbard Cable Looked Like When It Came Up from the Depths," NRK, May 26, 2022, https://www.nrk.no/tromsogfinnmark/this-is-what-the-damaged-svalbard-cable-looked-like-when-it-came-up-from-the-depths-1.16895904.

47 Atle Staalesen, "Someone Cut a Key Communications Cable to Norwegian Air Force Base," *Barents Observer*, August 23, 2024, https://www.thebarentsobserver.com/security/someone-cut-a-key-communications-cable-to-norwegian-air-force-base/165694#:~:text=The%20damage%20to%20the%20cable%20was%20discovered%20in%20April%20this,have%20been%20conducted%20with%20purpose.

48 "Telecoms Cable Break Reported Between Finland and Germany," YLE, November 18, 2024, https://yle.fi/a/74-20125339.

49 Miranda Bryant and Pjotr Sauer, "Swedish Police Focus on Chinese Ship After Suspected Undersea Cable Sabotage," *Guardian*, November 20, 2024, https://www.theguardian.com/world/2024/nov/20/sweden-denmark-undersea-cable-sabotage-navy-investigation; Bojan Pancevski, "Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables," *Wall Street Journal*, November 29, 2024, https://www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1.

50 "Joint Statement by the Foreign Ministers of Finland and Germany on the Severed Undersea Cable in the Baltic Sea," German Federal Foreign Office, November 18, 2024, https://www.auswaertiges-amt.de/en/newsroom/news/-/2685132.

51 Laura Pitel, Richard Milne, and Raphael Minder, "Severing of Baltic Sea Cables Likely to Be Sabotage, Germany Says," *Financial Times*, November 19, 2024, https://www.ft.com/content/33cd110b-e071-4b97-9af6-b6bde261515a.

52 Charlie Duxbury and Claudia Chiappa, "Northern Europe's New Naval Priority: Submarine Sabotage," POLITICO, January 2, 2024, https://www.politico.eu/article/northern-europe-naval-priority-submarine-sabotage/.

53 "The United States and Europe. A Concrete Agenda for Transatlantic Cooperation on China," United States Senate Committee on Foreign Relations, November 2020, 91, https://www.foreign.senate.gov/imo/media/doc/SFRC_Majority_China_Europe_Report_FINAL_P_and_G.pdf.

54 "Submarine Cable Map," TeleGeography, https://www.submarinecablemap.com/submarine-cable/peace-cable.

55 Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023), 183–220.

56 Laurens Cerulus and Sarah Wheaton, "How Washington Chased Huawei Out of Europe," POLITICO, November 23, 2022, https://www.politico.eu/article/us-china-huawei-europe-market/.

57 Jörn Fleck, Josh Lipsky, and David O. Shullman, "Ursula von der Leyen Set Europe's 'De-Risking in Motion. What's the Status One Year Later?," Atlantic Council, April 7, 2024, https://www.atlanticcouncil.org/blogs/new-atlanticist/ursula-von-der-leyen-set-europes-de-risking-in-motion-whats-the-status-one-year-later/.

58 "Security and Defence Implications of China's Influence on Critical Infrastructure in the European Union," European Parliament, January 17, 2024, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_EN.html.

59 Anne Kauranen and Andrius Sytas, "China Ship Is Focus of Pipeline Damage Probe, Finland Says," Reuters, October 20, 2023, https://www.reuters.com/world/finland-contacts-china-russia-regarding-baltic-sea-pipeline-investigation-2023-10-20/.

60 Finbarr Bermingham, "Beijing Admits Hong Kong-Flagged Ship Destroyed Key Baltic Gas Pipeline 'By Accident'," *South China Morning Post*, August 12, 2024, https://www.scmp.com/news/china/diplomacy/article/3274120/china-admits-hong-hong-flagged-ship-destroyed-key-baltic-gas-pipeline-accident.

61 Andrius Sytas and Essi Lehto, "Estonia Says Chinese Ship Is Main Focus of Probe Into Cables Damage," Reuters, November 10, 2023, https://www.reuters.com/world/europe/estonia-says-chinese-ship-is-main-focus-probe-into-cables-damage-2023-11-10/.

62 "Diplomat: China Still Stalling Over Balticconnector Legal Assistance Request," ERR, November 12, 2024, https://news.err.ee/1609519600/diplomat-china-still-stalling-over-baltconnector-legal-assistance-request.

63 Anna Pihl, "New Balticconnector Pipeline Damage Facts Come to Light," ERR, September 25, 2024, https://news.err.ee/1609470556/new-balticconnector-pipeline-damage-facts-come-to-light; and "National Bureau of Investigation Has Clarified Technically the Cause of Gas Pipeline Damage," Police of Finland, October 24, 2023, https://poliisi.fi/en/-/national-bureau-of-investigation-has-clarified-technically-the-cause-of-gas-pipeline-damage.

64 Forsvaret, Twitter post, November 20, 2024, https://x.com/forsvaretdk/status/1859195509866381402; Viktor Hedlund, "Kustbevakningen följer det kinesiska fartyget" [The coast guard is following the Chinese vessel], *Expressen*, November 23, 2024, https://www.expressen.se/nyheter/sverige/kustbevakningen-foljer-det-kinesiska-fartyget/.

65 "Convention for the Protection of Submarine Telegraph Cables," Article 10.

66 Bojan Pancevski, Sune Engel Rasmussen, and Benoit Faucon, "Chinese-Registered Ship Is Held in Baltic Sea Sabotage Investigation," *Wall Street Journal*, November 20, 2024, https://www.wsj.com/world/europe/chinese-registered-ship-is-held-in-baltic-sea-sabotage-investigation-27929472.

67 "U.S.-EU Trade and Technology Council Inaugural Joint Statement," White House, September 29, 2021, https://www.thebarentsobserver.com/security/someone-cut-a-key-communications-cable-to-norwegian-air-force-base/165694#:~:text=The%20damage%20to%20the%20cable%20was%20discovered%20in%20April%20this,have%20been%20conducted%20with%20purpose.

68 "U.S.-EU Joint Statement of the Trade and Technology Council," White House, December 5, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/#:~:text=On%20May%2016%2C%202022%2C%20at,physical%20prototype%20developed%20by%20industry; and U.S.-EU Joint Statement of the Trade and Technology Council," White

House, May 31, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/.

69 "One Step Forward, Two Steps Back: A Review of U.S.-Europe Cooperation on China," United States Senate Committee on Foreign Relations, Minority Staff Report, July 2024, https://www.foreign.senate.gov/imo/media/doc/risch_july_2024_one_step_forward_two_steps_back_a_review_of_useuropecooperationonchina.pdf.

70 "The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World," European Commission, September 26, 2024, https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world.

71 Sam Clark, "The West Has a Plan to Keep China, Russia Out of Subsea Data Pipes," POLITICO, September 12, 2024, https://www.politico.eu/article/china-russia-submarine-data-cables-security-united-states-european-union/.

72 "Norge slutter seg til internasjonalt initiativ om undersjøiske kabler" [Norway joins the International Initiative on Submarine Cables], Government of Norway, November 19, 2024, https://www.regjeringen.no/no/aktuelt/norge-slutter-seg-til-internasjonalt-initiativ-om-undersjoiske-kabler/id3075280/.

73 Edward Wong, "In Dealing With China, U.S. and Europe Take Different Tacks," *New York Times*, April 7, 2023, https://www.nytimes.com/2023/04/07/us/politics/china-us-europe.html; Paul Haenle, Chan Heng Chee, Liu Yawei, and Dan Baer, "Is Europe Aligned on China?," Carnegie Endowment for International Peace, May 9, 2023, https://carnegieendowment.org/posts/2023/05/is-europe-aligned-on-china?lang=en; and Alberto Nardelli, Jorge Valero, and Craig Trudell, "EU to Impose Tariffs Up to 45% on Chinese Electric Vehicles," Bloomberg, October 4, 2024, https://www.bloomberg.com/news/articles/2024-10-04/eu-votes-to-impose-tariffs-of-up-to-45-on-china-made-evs.

74 Francesca Ghiretti, "Profiling Relations of European Countries With China," Mercator Institute for China Studies, October 31, 2023, https://merics.org/en/profiling-relations-european-countries-china; and Rebecca Arcesati and Tobias Gehrke, "Europe's Economic Security Agenda Needs Far Better Techno-Industrial Intelligence," Mercator Institute for China Studies, October 28, 2024, https://merics.org/en/comment/europes-economic-security-agenda-needs-far-better-techno-industrial-intelligence.

75 "One Step Forward, Two Steps Back," 80.

76 Submarine Telecoms Forum, "Industry Report, 2023–2024: Issue 12," 2023, https://issuu.com/subtelforum/docs/submarine_telecoms_industry_report_issue_12, 104; and Oliver Pinaud, "Big Tech Colonizes Seabed."

77 Clothilde Goujard and Laurens Cerulus, "Inside Gaia-X: How Chaos and Infighting Are Killing Europe's Grand Cloud Project," POLITICO, October 26, 2021, https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/.

78 Pinaud, "Big Tech Colonizes Seabed."

79 Mario Draghi, "The Future of European Competitiveness—A Competitiveness Strategy for Europe," European Commission, September 9, 2024, 30, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

80 Submarine Telecoms Forum, "Industry Report, 2024–2025: Issue 13," 74.

81 Laura Zhou, "The Heated US-China Cable Competition Under the Seas," *South China Morning Post*, November 1, 2024, https://www.scmp.com/news/china/science/article/3284708/heated-us-china-cable-competition-under-seas?module=perpetual_scroll_0&pgtype=article.

82 "Staid Aid Overview," European Commission, https://competition-policy.ec.europa.eu/state-aid/overview_en.

83 Ursula von der Leyen, "Mission Letter to Teresa Ribera Rodríguez," European Commission, September 17, 2024, 6, https://commission.europa.eu/document/download/5b1aaee5-681f-470b-9fd5-aee14e106196_en?filename=Mission%20letter%20-%20RIBERA.pdf.

84 Anna Desmarais, "Officials Are Worried About Internet Blackouts. How Vulnerable Are Underwater Cables to Attacks?," *Euronews*, September 21, 2024, https://www.euronews.com/next/2024/09/21/officials-are-warning-about-the-vulnerability-of-underwater-cables-how-protected-are-they.

85 "Europeans Wade Into Fighting Seabed Threats With Drones and Sensors," DefenseNews, January 9, 2023, https://www.defensenews.com/global/europe/2023/01/09/europeans-wade-into-fighting-seabed-threats-with-drones-and-sensors/.

86 Christian Bueger, "NATO's Contribution to Critical Maritime Infrastructure Protection," Center for Maritime Strategy, January 19, 2024, https://centerformaritimestrategy.org/publications/natos-contribution-to-critical-maritime-infrastructure-protection/.

87 Cooper, "NATO Warns Russia Could Target Undersea Pipelines and Cables."

88 Alexandra Brzozowski, "NATO Seeks Ways of Protecting Undersea Cables From Russian Attacks," Euractiv, October 23, 2020, https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/; and "Vilnius Summit Communiqué," North Atlantic Treaty Organization, July 11, 2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

89 "NATO Defence Ministers Launch Initiative to Enhance Maritime Surveillance Capabilities," North Atlantic Treaty Organization, October 12, 2023, https://www.nato.int/cps/en/natohq/news_219441.htm; and "NATO and Industry Work Together to Strengthen Maritime Surveillance," North Atlantic Treaty Organization, April 17, 2024, https://www.nato.int/cps/en/natohq/news_224798.htm?selectedLocale=en.

90 "NATO Exercises With New Maritime Unmanned Systems in Portugal," North Atlantic Treaty Organization, September 19, 2023, https://www.nato.int/cps/en/natohq/news_218545.htm; and "NATO's Digital Ocean Initiative Gets a Boost in Portugal," North Atlantic Treaty Organization, September 20, 2024, https://www.nato.int/cps/en/natohq/news_228959.htm?selectedLocale=en.

91 Natalia Ojewska, "Tusk Proposes Navy Policing in Baltic Sea Amid Russia Threat," Bloomberg, November 27, 2024, https://www.bloomberg.com/news/articles/2024-11-27/tusk-proposes-navy-policing-in-the-baltic-sea-amid-russia-threat.

92 Vivienne Machi, "French Military Tees Up New Tech in Rush to Conquer the Seabed," DefenseNews, February 14, 2022, https://www.defensenews.com/global/europe/2022/02/14/french-military-tees-up-new-tech-in-rush-to-conquer-the-seabed/; and "Seabed Warfare Strategy: Report by the Working Group," Ministère des Armées, February 2022, https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf.

93 "Exail Selected by French Defense Procurement Agency to Develop the French Navy's Ultra-Deepwater AUV," Exail, October 3, 2024, https://www.exail.com/exail-selected-by-french-defense-procurement-agency-to-develop-the-french-navys-ultra-deepwater-auv/.

94 Greg Noone, "Could Undersea Cables Be the Next Casualty of Hybrid Warfare?" *New Statesman*, March 10, 2023, https://www.newstatesman.com/spotlight/tech-regulation/cybersecurity/2023/03/akademik-boris-petrov-russia-undersea-cables-next-casualty-hybrid-warfare.

95 George Allison, "Britain's New Undersea Cable Protection Ship Arrives," UK Defence Journal, January 19, 2023, https://ukdefencejournal.org.uk/britains-new-undersea-cable-protection-ship-arrives/.

96 Ibid.

97 "Nevers Call to Reinforce the EU's Cybersecurity Capabilities," French Presidency of the Council of the European Union, March 9, 2022, https://lvm.fi/en/-/eu-telecommunications-ministers-initiate-action-to-combat-disinformation-and-improve-cyber-security-1684637.

98 "Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)," European Commission, December 14, 2022, https://eur-lex.europa.eu/eli/dir/2022/2555.

99 "EU-NATO Task Force on the Resilience of Critical Infrastructure. Final Assessment Report," European Commission and North Atlantic Treaty Organization, June 2023, https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf.

100 "Recommendation on the Security and Resilience of Submarine Cable Infrastructures," European Commission, February 21, 2024, https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures.

101 "The New York Joint Statement."

102 Author interview with an EU Official, May 2023.

103 Jill C. Gallagher, "Undersea Telecommunication Cables: Technology Overview and Issues for Congress," Congressional Research Service, September 13, 2022, 14–15, https://crsreports.congress.gov/product/pdf/R/R47237.

104 Luca Bertuzzi, "EU Countries Lay Bare Europe's Limits in Securing Critical Infrastructure," Euractiv, November 3, 2022, https://www.euractiv.com/section/digital/news/eu-countries-lay-bare-europes-limits-in-securing-critical-infrastructure/.

105 Umbach, "New Challenges."

106 "NATO Stands Up Undersea Infrastructure Coordination Cell," North Atlantic Treaty Organization, February 15, 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.

107 "NATO and European Union Launch Task Force on Resilience of Critical Infrastructure," North Atlantic Treaty Organization, March 16, 2023, https://www.nato.int/cps/en/natohq/news_212874.htm.

108 "Joint Statement by Joint Expeditionary Force Ministers, June 2023," UK Ministry of Defence, June 13, 2023, https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-june-2023.

109 Melisa Čavčić, "After Pipeline Incident, JEF Partners Pool Resources for Subsea Infrastructure Protection in Baltic Sea," Offshore Energy, December 5, 2023, https://www.offshore-energy.biz/after-pipeline-incident-jef-partners-pool-resources-for-subsea-infrastructure-protection-in-baltic-sea/.
110 "Six North Sea Countries Join Forces to Secure Critical Infrastructure," Government of Norway, April 9, 2024, https://www.regjeringen.no/contentassets/03b6ba0be17e4ea0a57517a771ab5d8b/20240409_press-release_six-north-sea-countries-join-forces-to-secure-critical-infrastructure.pdf.
111 Detsch and Johnson, "NATO Wants to Boost Its Undersea Defenses"; and "Norway's Gassco Keeps Eye on Security Situation After Balticconnector Damage," S&P Global, October 13, 2023, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/natural-gas/101323-norways-gassco-keeps-eye-on-security-situation-after-balticconnector-damage.
112 "Harbour & Maritime Surveillance and Protection (HARMSPRO)," Permanent Structured Cooperation, https://www.pesco.europa.eu/project/harbour-and-maritime-surveillance-and-protection/.
113 "Critical Seabed Infrastructure Protection (CSIP)," Permanent Structured Cooperation, https://www.pesco.europa.eu/project/critical-seabed-infrastructure-protection-csip/.
114 Katrina Manson, "NATO Backs Effort to Save Internet by Rerouting to Space in Event of Subsea Attacks," Bloomberg, July 8, 2024, https://www.bloomberg.com/news/articles/2024-07-08/nato-backs-effort-to-reroute-internet-to-space-in-event-of-subsea-attacks.
115 Anna Gross, Alexandra Heal, Chris Campbell, Dan Clark, Ian Bott, et al., "How the US Is Pushing China Out of the Internet's Plumbing," *Financial Times*, June 13, 2023, https://ig.ft.com/subsea-cables/.
116 David Sacks, "Will the U.S. Plan to Counter China's Belt and Road Initiative Work?," Council on Foreign Relations, September 14, 2023, https://www.cfr.org/blog/will-us-plan-counter-chinas-belt-and-road-initiative-work.
117 Michele Barbero, "Europe Is Trying (and Failing) to Beat China at the Development Game," *Foreign Policy,* January 10, 2023, https://foreignpolicy.com/2023/01/10/europe-china-eu-global-gateway-bri-economic-development/.
118 Emmanuel Martin, "The Paradoxes of the EU's Africa Policy," GIS Reports Online, June 28, 2024, https://www.gisreportsonline.com/r/eu-africa-strategy/.
119 "About Connecting Europe Facility—Digital," European Health and Digital Agency, https://hadea.ec.europa.eu/programmes/connecting-europe-facility/about_en.
120 "Call for Proposals: CEF Digital—Backbone Connectivity for Digital Global Gateways," European Health and Digital Executive Agency, October 22, 2024, 6, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/cef/wp-call/2024/call-fiche_cef-dig-2024-gateways_en.pdf.
121 "Connecting Europe Facility (CEF)—Multiannual Work Programme 2024–2027," European Commission, October 9, 2024, https://digital-strategy.ec.europa.eu/en/library/connecting-europe-facility-cef-multiannual-work-programme-2024-2027.
122 Luca Bertuzzi, "EU Readies Second Round of Submarine Cables Financing, but Resource Allocation Raises Questions," Euractiv, October 18, 2023, https://www.euractiv.com/section/digital/news/eu-readies-second-round-of-submarine-cables-financing-but-resource-allocation-raises-questions/.
123 "Call for Proposals."
124 Bertuzzi, "EU Readies Second Round of Submarine Cables Financing, but Resource Allocation Raises Questions."
125 Ibid.
126 Isabelle Bousquette, "A Warming Arctic Emerges as a Route for Subsea Cables," *Wall Street Journal*, June 15, 2022, https://www.wsj.com/articles/a-warming-arctic-emerges-as-a-route-for-subsea-cables-11655323903.
127 Mathieu Pollet and Giovanna Coi, "Shrinking Arctic Ice Redraws the Map for Internet Cable Connections," POLITICO, April 2, 2024, https://www.politico.eu/article/shrinking-arctic-ice-redraws-map-internet-cable-connections-climate-change/.
128 Alexandra Heal and Anna Gross, "EU Plans Black Sea Internet Cable to Reduce Reliance on Russia," *Financial Times*, May 12, 2023, https://www.ft.com/content/d07dbd19-5e8b-4543-85f6-bbf1a6a0858d.
129 "World Leaders Launch a Landmark India-Middle East-Europe Economic Corridor," White House, September 9, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/09/fact-sheet-world-leaders-launch-a-landmark-india-middle-east-europe-economic-corridor/.
130 Alberto Rizzi, "The Infinite Connection: How to Make the India-Middle East-Europe Economic Corridor Happen," European Council on Foreign Relations, April 23, 2024, https://ecfr.eu/publication/the-infinite-connection-how-to-make-the-india-middle-east-europe-economic-corridor-happen/.

131 "U.S.-EU Joint Statement of the Trade and Technology Council," White House, April 5, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/05/u-s-eu-joint-statement-of-the-trade-and-technology-council-3/.
132 Bertuzzi, "EU Countries Lay Bare Europe's Limits in Securing Critical Infrastructure."
133 "Baltic Air Policing," North Atlantic Treaty Organization Allied Air Command, https://ac.nato.int/missions/air-policing/baltics.
134 "European Union and NATO hold the first Structured Dialogue on Cyber," European Union External Action Service, October 4, 2024, https://www.eeas.europa.eu/eeas/european-union-and-nato-hold-first-structured-dialogue-cyber-0_en.
135 Tara Davenport, "Intentional Damage to Submarine Cable Systems by States," Hoover Institution, Stanford University, October 26, 2023, 6.
136 "One Step Forward, Two Steps Back," 80.
137 Joseph B. Keller, "The Disconnect on Undersea Cable Security," Lawfare, May 7, 2023, https://www.lawfaremedia.org/article/the-disconnect-on-undersea-cable-security.
138 "One Step Forward, Two Steps Back," 81.
139 "Call for Proposals."
140 Bafoutsou, Papaphilippou, and Dekker, "Subsea Cables—What Is at Stake?," 8.
141 "EU-India Trade and Technology Council," European Parliamentary Research Service, January 2024, https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757587/EPRS_ATA(2024)757587_EN.pdf.

Carnegie Endowment for International Peace

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 170 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

Europe Program

The Europe Program in Washington explores the political and security developments within Europe, transatlantic relations, and Europe's global role. Working in coordination with Carnegie Europe in Brussels, the program brings together U.S. and European policymakers and experts on strategic issues facing Europe.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org