

Safeguarding Subsea Cables

Protecting Cyber Infrastructure amid Great Power Competition

By Daniel Runde, Erin Murphy, and Thomas Bryja

Subsea fiber-optic cables, a critical information and telecommunications technology (ICT) infrastructure carrying more than 95 percent of international data, are becoming a highly consequential **theater of great power competition** between the United States, China, and other state actors such as Russia. The roughly **600 cables planned** or currently operational worldwide, spanning approximately **1.2 million kilometers**, are the world's **information superhighways** and provide the high-bandwidth connections necessary to support the rise of cloud computing and integrated 5G networks, transmitting everything from streaming videos and financial transactions to diplomatic communications and essential intelligence. The demand for data center computing and storage resources is also expected to increase in the wake of the artificial intelligence revolution. Training large language models takes enormous, distributed storage to compute, and if those networks are globally oriented, they will require additional subsea capacity to connect them. These geopolitical and technological stakes necessitate a consideration of the vulnerabilities of subsea systems and the steps the United States can take to fortify the digital rails of the future and safeguard this critical infrastructure.

Undersea Cables: Why Do They Matter?

Subsea cables are critical for nearly all aspects of commerce and business connectivity. For example, one major international bank moves an average of **\$3.9 trillion** through these cable systems every workday. Cables are the backbone of global telecommunications and the internet, given that user data (e.g., e-mail, cloud drives, and application data) are often stored in data centers around the world. This infrastructure effectively facilitates daily personal use of the internet and broader societal functions. In addition, sensitive government communications also rely extensively on subsea infrastructure. While these communications are encrypted, they still pass through commercial internet lines as data traverses subsea infrastructure. Subsea cables carry a much larger bandwidth and are **more efficient**,

cost-effective, and reliable than satellites; consequently, they **have been credited** with increasing access to high-speed internet worldwide, fueling economic growth, boosting employment, enabling innovation, and lowering barriers to trade. These networks are now indispensable links for the modern world and are pivotal to global development and digital inclusivity.

Cable Laying, Ownership, and Control

Undersea cables are **built, owned, operated, and maintained** primarily by private sector companies. Approximately 98 percent of the world’s undersea cables are manufactured and installed by four private firms: in 2021, the U.S. company **SubCom**, French firm **Alcatel Submarine Networks (ASN)**, and Japanese firm **Nippon Electric Company (NEC)** collectively held an **87 percent market share**, with China’s **HMN Technologies**, formerly known as Huawei Marine Networks Co., Ltd., holding another 11 percent. Commercial undersea cables can be owned by a single company or a consortium of companies, including telecommunication providers, undersea cable companies, content providers, and cloud computing service providers. Amazon, Google, Meta, and Microsoft now own or lease **around half** of all undersea bandwidth worldwide. The companies that build and own these cables often lease out bandwidth on their cables through **indefeasible rights of use (IRUs)**, which grant long-term access to a portion of the cable’s capacity. IRU holders can also lease this bandwidth to other third parties, creating a layered leasing market that extends the cable’s reach and utility across various sectors and regions.

China’s rapid emergence as a **leading subsea cable provider and owner** has been the centerpiece of Beijing’s ambitious **Digital Silk Road** initiative launched in 2015, which aims to capture **60 percent** of the global fiber-optic cable market by targeting emerging economies in Asia, Africa, the Middle East, and the Pacific. While Chinese companies have been **recently blocked** from subsea cable projects involving U.S. investment and firms due to U.S. concerns about the national security risks that come with HMN Technologies’ unbridled growth, the company has provided **18 percent** of the subsea cables (in terms of the total length of cable) that have been laid worldwide over the past four years. HMN Technologies has also become the world’s **fastest-growing** subsea cable builder over the past 10 years. A 2020 Federal Communications Commission (FCC) **report** referenced the fact that HMN Technologies has “built or repaired” almost 25 percent of subsea cables and is due to build only 7 percent of the cables currently under development globally, perhaps indicating a potential trend of the Chinese firm’s slowing control over international cable construction.

The Vulnerability of Cable Systems and the Potential for Chinese Exploitation

Undersea cables can be highly vulnerable to a variety of factors. **Most cable damage** is unintentional, mainly stemming from accidental human interaction with the cables. Still, potential hazards to the cables range from anchoring and fishing equipment to extreme weather such as earthquakes and landslides. Damage to submarine cables is **relatively common**—an estimated 100 to 150 cables are severed each year—mostly from fishing equipment or anchors.

The scale and exposure of undersea infrastructure also make it an easy target for saboteurs operating in the gray zone of **“deniable attacks short of war.”** In 2023, Taiwanese authorities accused two Chinese vessels in the area of **cutting** the only two submarine cables that supply internet to Taiwan’s Matsu Islands, plunging its 14,000 residents into digital isolation for six weeks. Although there was **no**

The scale and exposure of undersea infrastructure also make it an easy target for saboteurs operating in the gray zone of “deniable attacks short of war.”

clear confirmation of a deliberate attack, Taiwan’s ruling Democratic Progressive Party (DPP) pointed to a remarkable **frequency of Chinese vessels causing cable disruptions—27 times** since 2018—and **accused Beijing** of harassing Taiwan in a classic case of “gray-zone aggression.” Similarly, in October 2023, a Baltic Sea **telecom cable** connecting Sweden and Estonia sustained damage at the same time as a Finnish-Estonian gas pipeline and cable. Carl-Oskar Bohlin, Sweden’s minister for civil defense, said the Swedish-Estonian cable was damaged as a result of “**external force or tampering**” and that Estonian officials had concluded that the three incidents were “related.” An **investigation** focused on a Russian-flagged ship and a Chinese-owned vessel operating in the area as the likely sources of the alleged sabotage. Private cable firms have also identified the South China Sea and the Red Sea as two notable choke points in the international undersea cable network. In the Red Sea, a spate of **Houthi attacks** has indirectly damaged cables in this major artery connecting Europe and Asia.

Less likely, but still of concern, geopolitical rivals such as China could potentially collect the data flowing through this infrastructure. U.S. officials have **sounded the alarm** over the involvement of Chinese firms in new global seabed cable projects, suggesting that China could **monitor data** running through the cables or even sever entire countries from the internet either through software or interfering at coastal landing stations for the cables. As concerns grow over Chinese delays with granting permits, challenges facing cable repair, and even the potential of state tampering with cables, U.S. and allied-country companies have rerouted planned subsea cable systems away from landing in Chinese territories and other vulnerable areas. For example, the U.S. government and the **Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector**, also known as “Team Telecom,” **denied** issuing a submarine cable license for the Pacific Light Cable Network (PLCN) system that was meant to connect the United States with Hong Kong, **citing** “national security and foreign ownership concerns” with the direct connection to China-controlled Hong Kong. However, the segments of the PLCN system that were already going to land in Taiwan and the Philippines were still approved. Two other applications for planned cable systems that connected with Hong Kong were withdrawn and redesigned due to similar national security considerations. At the same time, Chinese authorities in recent years have been **delaying approval or denying the use of subsea cables altogether** that would move through the South China Sea. China’s territorial claim over the South China Sea has prevented the subsea cable industry from accessing the region for north-south connectivity in the Pacific.

Another backdoor vulnerability is the challenge of high-risk vendors. While a trusted supplier may install subsea cables, they can be maintained by a repairer from a high-risk vendor, some of whom are Chinese. The overreliance on Chinese repair ships due to limited alternatives in the marketplace is another vulnerability if, during a time of military conflict, the Chinese government prohibits access to its repair ships and subsea cables are left damaged without timely repair. Therefore, U.S. and allied officials have warned that the repair and maintenance process of undersea cables in the Pacific Ocean makes them even more **vulnerable to espionage** from the Chinese Communist Party (CCP) or other

The overreliance on Chinese repair ships due to limited alternatives in the marketplace is another vulnerability if, during a time of military conflict, the Chinese government prohibits access to its repair ships and subsea cables are left damaged without timely repair.

state actors. State-controlled Chinese company S.B. Submarine Systems (SBSS) repairs international undersea cables, including those owned by U.S. companies such as Google and Meta, and it appears that SBSS has been **hiding its vessels' locations** from radio- and satellite-tracking services without plausible explanation while operating off Taiwan, Indonesia, and other coasts in Asia. There are



This regional snapshot of the web of subsea cables in the Indo-Pacific displays at once both the interdependence and vulnerability of these systems.

Source: Submarine Cable Map 2024/TeleGeography

concerns that Chinese cable repair companies such as SBSS could tap undersea data streams, map the ocean floor to conduct reconnaissance on U.S. military communication links, or obtain highly specific location data from the internal documentation of cable systems that would allow belligerent parties to cut cables with speed and precision.

Russian Threats to Undersea Infrastructure

While the international focus in this theater has largely been on the competition between the United States and China, **Russian threats** to subsea infrastructure are their own significant concern. Russia relies significantly less on subsea cables than either the United States or China due to its position as a continental power with internet connectivity to Europe and Central Asia and less of a focus on international trade. This makes Russia less vulnerable to disruptions in subsea cable infrastructure and potentially more willing to **exploit these vulnerabilities** in other nations. **Recent activity by Russian naval and intelligence assets**, including the spy ship *Yantar* and specialized submarines such as the *Losharik*, has raised alarm among Western defense and security officials. *Yantar*, for instance, has been observed **loitering near undersea cable routes**, equipped with submersibles capable of cutting or tapping into these cables, signaling a clear intent to exploit these vulnerabilities in a potential conflict scenario.

The strategic importance of undersea cables has not been lost on Russia, which views this infrastructure as a critical point of leverage against the security of Western nations. This perspective is emphasized in statements from high-ranking Russian officials such as Dmitry Medvedev, deputy chairman of Russia's Security Council, who, following the Nord Stream pipeline explosions in 2023, indicated that Russia **could target** undersea communication cables as retaliation for alleged Western involvement in the blasts. This rhetoric, coupled with physical evidence of Russian activities near this vital infrastructure, has brought about **concerns** within NATO and allied nations about the potential for Russian sabotage aimed at disrupting Western economies and communications in times of heightened tensions or outright conflict.

The strategic importance of undersea cables has not been lost on Russia, which views this infrastructure as a critical point of leverage against the security of Western nations.

The capacity for such sabotage is backed by Russia's significant investment in specialized capabilities for deep-sea operations. The Main Directorate for Deep Sea Research, a unit within the Russian Ministry of Defense, operates several **advanced submarines**, such as the titanium-hulled *Losharik*, capable of operating at extreme depths and equipped with manipulator arms for interacting with undersea infrastructure. These capabilities are not solely offensive; they also include the ability to place sensors and remove foreign surveillance equipment, adding a layer of complexity to Russia's undersea operations. The **dual-use nature** of these assets—intended for intelligence gathering and potential sabotage—illustrates the multifaceted threat they pose to global undersea infrastructure.

NATO has responded to this threat by increasing **surveillance and protection efforts** around critical undersea infrastructure. NATO's **Allied Maritime Command** has identified an increase in Russian

naval activity, including around the North and Baltic Seas, home to numerous vital undersea cables. Vice Admiral Didier Maletierre, deputy commander of Allied Maritime Command, highlighted that Russian nuclear-powered submarines, specifically designed for hybrid warfare, have been developed to **target this infrastructure**. The alliance has boosted patrols and established a **Critical Undersea Infrastructure Coordination Cell** to build cooperation with private sector entities and improve monitoring and response capabilities, further emphasizing the serious nature of the threat.

Recommendations to Counter Undersea Great Power Competition

- **It is critical that the United States and its allies leverage development finance institutions (DFIs), multilateral development banks (MDBs), export credit agencies (ECAs), government agencies, and the private sector to support host countries and help U.S. and allied firms compete with their Chinese and Russian counterparts and secure allied systems.** Subsea cable projects are expensive. The cost varies from \$30,000 to \$50,000 per kilometer for subsea communication cables. Even though HMN Technologies (formerly Huawei Marine Networks Co., Ltd.) is still perceived as offering **lower-quality** technology than its competitors, it can offer dramatically cheaper contracts than Western firms can afford. HMN Technologies' bids to work on undersea cables projects are priced **20 to 30 percent lower** than its rivals, which could help China secure more deals moving forward. For now, U.S. government campaigns have successfully **thwarted Chinese companies** from winning contracts where U.S. companies were also bidders.

For example, the United States successfully ousted HMN Technologies from the Southeast Asia-Middle East-Western Europe 6 (SMW6) subsea fiber-optic cable system, which links Singapore to France. To do so, the United States used both **sweeteners** and **warnings**. The U.S. Trade and Development Agency offered training grants valued at a total of \$3.8 million to five telecommunications companies involved in the selection process and located in countries on the cable route. This offer was conditional on them choosing the U.S. firm SubCom as the supplier. The U.S. Export-Import Bank (EXIM) also **extended support** to SubCom. SubCom won the \$600 million contract for SMW6 by offering specifically designed training assistance. SubCom landed the contract also thanks to the work of U.S. diplomats, who warned foreign telecommunications carriers about the security risks surrounding HMN Technologies and the crippling sanctions that the United States was planning to impose on the Chinese company, putting their investment at significant risk. This bilateral U.S. diplomatic effort helped SubCom ultimately win the contract.

The United States is also financing undersea cables in strategic areas such as the Indo-Pacific, one of the primary theaters of geopolitical competition between the United States and China. In that region, the U.S. International Development Finance Corporation (DFC) **committed** to providing a loan of up to **\$190 million** to Trans-Pacific Networks, who partnered with Telstra International, to support the construction of a 15,200 km submarine fiber-optic cable connecting Singapore, Indonesia, and the United States. The new cable will expand and enhance internet access across the region, including to isolated Pacific islands.

The United States is also financing undersea cables in strategic areas such as the Indo-Pacific, one of the primary theaters of

geopolitical competition between the United States and China.

DFIs, such as the DFC, and MDBs, such as the World Bank and Asian Development Bank, also provide essential funding, risk mitigation, and project development capabilities that enable U.S. and allied companies to compete against Chinese state-subsidized firms. The DFC's ability to operate in middle- and upper-middle-income countries can be improved by increasing its investment cap, which currently stands at **\$60 billion**. These institutions can also offer loans and guarantees, reducing financial risks for large-scale infrastructure projects. ECAs, including EXIM and the Japan Bank for International Cooperation, play a **crucial role** in supporting the development of trusted undersea cable infrastructure by providing insurance and credit facilities that protect against political and commercial risks. This financial backing is vital for developing and maintaining undersea cables, ensuring that this critical infrastructure remains under the control of trusted entities. **Greater coordination** between these financial bodies will ultimately lead to more effective resource allocation and risk management.

- **The United States should lessen the vulnerabilities of subsea cables by building repair capacity, increasing funding for cable ship repairs, and streamlining the permitting process, improving the security and resilience of cable networks.** The global fiber-optic network is **designed** with a certain level of redundancy to handle frequent damage. Most countries are linked by multiple underwater cables, enabling data to be redirected smoothly if one or two lines are affected. However, repairing is complex, costly, and time consuming in the event of **more significant damage**. According to the **International Cable Protection Committee (ICPC)**—an organization that promotes the safeguarding of submarine cables, facilitates collaboration among industry and government stakeholders, and whose more than **215 members** own 98 percent of the world's undersea cables—cable repairs average between \$1 and \$3 million, require “specialized cable ships with highly trained crews that cost tens of thousands of dollars per day,” and can take months to complete. Submarine internet cable provider Seacom reported that repairing the damaged Red Sea cables would take **at least eight weeks** due to the permitting requirements needed to begin the process. Restoration costs sometimes **exceed repair costs** due to the need to reroute communications over unimpaired systems.

To reduce the vulnerability of critical cable systems, the United States should consider increasing current federal funding to augment the industrial base for U.S. cable repair, deployment, and maintenance. The **Cable Security Fleet (CSF)**, implemented in 2021 and modeled after the Maritime Security Program, is a federal infrastructure protection program—partly overseen by the Pentagon—meant to address the lack of rapid response and repair capacity of U.S. ships in case of a national emergency or war. SubCom, one of the world's **largest** subsea fiber-optic cable developers for telecommunication and technology firms and the **sole cable contractor for the U.S. military**, was awarded a **\$10 million annual contract** in 2021 by the U.S. Department of Transportation to operate the CSF. The CSF consists of two U.S.-flagged and crewed cable ships, the *CS Dependable* and *CS Decisive*, which are required to be available for laying, maintaining, and repairing critical cables. The CSF funding requires an **annual appropriation by Congress**,

as each ship operator receives a \$5 million stipend annually if the ship meets contractual and statutory requirements.

Enhancing the resilience of submarine communications cable systems **would involve** increasing redundancies, introducing more cables with greater carrying capacity, and improving capabilities to promptly maintain and repair cable systems. The supply chain for many of the components of cable systems is global. For instance, optical and power components for undersea repeaters are manufactured in China and some Southeast Asian nations. Securing a good supply chain is also essential to ensure that cables from ASN, NEC, and SubCom can be manufactured (and spares can be manufactured for existing cables). Given the costs associated with the installation of more cables with greater carrying capacity, prompt repair capabilities provide a **more effective method** of introducing resilience in the cable system. This effort is complicated by the shortage of cable repair ships, especially given the rapid increase in subsea cables built over the past five years. The U.S. government and its allies should consider investing in the construction of new repair ships, as many existing vessels are aging and nearing retirement. The cost of a new cable ship can reach **over \$100 million**. But even with prompt repair capacity, there needs to be a “break glass” capability to deploy new cables rapidly. This would include classified cable route planning and surveys ahead of the need date so that there are no delays in initiating new cable deployments should existing routes be compromised. Regional capability to partially re-lay new systems destroyed due to massive intentional cuts would also enhance resiliency. The Tonga volcano **cuts** in 2022 are a good illustration of how long it takes to find new cables and create a solution, especially when a repeater is destroyed.

Enhancing the resilience of submarine communications cable systems would involve increasing redundancies, introducing more cables with greater carrying capacity, and improving capabilities to promptly maintain and repair cable systems.

Policymakers should ensure that domestic and **international legal and regulatory frameworks**, including permitting and liability regimes, are structured and operated to facilitate efficient and effective subsea cable repairs and installations while minimizing undue delays and costs. However, this efficiency cannot come at the cost of security, so the U.S. government and allies should not turn to untrusted repairers for speedy restoration. **Electronic monitoring systems** could enhance the physical and data security of subsea cables by detecting any changes or anomalies in the seabed environment and alerting operators. **Electronic protection** in the form of an end-to-end encryption system also reduces the risk of surveillance, tapping, and spying.

- **The U.S. government must prioritize developing and implementing a cohesive legal and international framework to defend the submarine cable network.** The current legal and international framework is complex and fragmented, with different **international legal regimes** determining responsibility and punishment for sabotage depending on where the

cables are laid. When cables are sabotaged in international waters, there is no regime to hold the perpetrator accountable. The United States is not even a signatory to the latest international treaties that address subsea cable protection. There also needs to be an increase in naval security from governmental bodies—in the event of war, there needs to be **greater capacity** to repair undersea fiber-optic cables in order to improve the United States’ wartime resilience. The United States could better leverage the **ICPC** to prevent damage, establish internationally recognized protections, and provide an apolitical forum for discussions about best practices, regulatory harmonization, data protection standards, and security measures. Participation in the ICPC may further the private-sector-led “**businesslike attitude**” toward cable building, repair, and maintenance; provide the architecture for international standards and practices and cooperative public-private management of critical communication infrastructure; and generate an environment to develop relationships with trusted vendors.

- **The United States should update its burdensome domestic permitting processes.** The United States lacks a comprehensive regulatory environment to streamline the issuance of cable permits. Under the Cable Landing License Act of 1921, all submarine cable operators must acquire a license from the **FCC**. For cables with significant foreign ownership or that connect the United States with foreign landing points, applications must be reviewed by the **Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector**. Cables must receive a federal permit from the Army Corps of Engineers to evaluate their potential impact on the environment and any endangered species, but if the cables are placed in **marine sanctuaries**, then the National Oceanic and Atmospheric Administration exercises authority. Yet if cables are dropped on the continental shelf, authority rests with the Federal Energy Regulatory Commission. These requirements are just at the federal level—excluding necessary state and local permits. Overall, the combined licensing processes can take up to two years. That is bad for business and good for the CCP’s cable suppliers. Rather than this jungle of jurisdictions and lengthy national security reviews, the United States might consider centralizing the monitoring of undersea cables under one agency in a way that coordinates existing actors and has the authority to streamline the approval process for cables as critical infrastructure. After all, according to a Communications Security, Reliability, and Interoperability Council **report**, “federal agencies often fail to coordinate among themselves and with their state and local counterparts on even an *ad hoc* basis to ensure submarine cable protection.” The United States is also unique in how burdensome its national security review and ongoing obligations are, creating strong disincentives to locate subsea cables in the United States. Greater transparency, speed, and uniformity, as well as the development of due process protections, are needed.
- **The United States should closely collaborate with its allies in two capacities: engaging in regulatory cooperation and providing technical assistance to developing countries and emerging economies.** The current state of the international regulatory framework is a major concern among industry leaders, as cable companies have repeatedly expressed frustration over the disparate processes in each country, which significantly extend the time required to obtain permits before construction can begin. Establishing an international body to help countries create uniform regulatory processes across the globe could streamline these efforts.

In 2019, Japan outlined the **Data Free Flow with Trust** (DFFT) concept, which promotes the free flow of data and the protection of individual privacy, national security, and intellectual property by connecting undersea cables only with allies and partner nations. At its May 2023 summit in Hiroshima, the G7 **endorsed** the creation of the Institutional Arrangement for Partnership, which puts the DFFT into action. In the same vein, the Quad—a strategic security dialogue between Australia, India, Japan, and the United States—launched the **Partnership for Cable Connectivity and Resilience** in 2023 to strengthen submarine cable systems in the Indo-Pacific by leveraging the four countries’ expertise in designing, manufacturing, laying, and maintaining undersea cables. Under this partnership, Australia will establish the Indo-Pacific Cable Connectivity and Resilience Program, which will commission technical and policy research frameworks in addition to providing technical assistance.

The United States, through the Quad 2023 partnership and its \$5 million **CABLES program**, will provide technical and capacity-building assistance on the security of undersea cables. Development agencies such as the U.S. Agency for International Development (USAID) have also emphasized the importance of fostering digital connectivity in developing countries, particularly in the Indo-Pacific region, and ensuring that these countries have the capacity to effectively implement and manage the undersea cables once they are landed. For example, USAID has been providing **technical assistance** to support the development of a \$30 million undersea cable spur that will connect Palau to the **DFC-financed** Singapore-U.S. cable—the longest in the world. The Palau cable spur is part of a larger U.S. government initiative to build greater telecommunications infrastructure throughout the Pacific islands, which, in turn, is meant to promote innovation, connectivity, and development throughout the region.

In parallel, in April 2024, Google **announced** an additional \$1 billion investment in digital connectivity as part of its Pacific Connect Initiative, which includes multiple cable systems it is building in the Pacific, specifically designed with branching units to connect Pacific island nations with little to no existing connectivity. This multilateral initiative by Google, which includes geopolitical collaboration from multiple governmental bodies, aligns with the U.S. government’s efforts and presents an opportunity for greater public-private partnerships in this space. The **Marea cable**, connecting Virginia with Spain and developed by Microsoft, Meta, and telecommunications company Telsius, is also part of a network of advanced cables that promotes digital connectivity, upgraded global internet infrastructure, and greater speed and resiliency. By collaborating with private sector leaders, the United States can further enhance its initiatives and make strides in bridging the digital divide around the world.

Conclusion

Undersea cables are critical to global communications infrastructure, supporting everything from financial transactions to national security communications, making them a prime target in the escalating great power competition between the United States, China, and Russia, as well as for other state and non-state actors. As the lifelines of the digital age, these cables support economic activities, military operations, and everyday internet usage. Thus, their security is paramount. The threats posed by state actors—particularly Russia and China—highlight the urgent need for measures to protect this infrastructure. Russia’s strategic use of specialized submarines and espionage vessels to potentially

sabotage undersea cables, combined with China's rapid expansion in subsea cable construction and control, underlines the vulnerability of these critical systems. Without coordinated international efforts to safeguard these cables, the risks of disruption, espionage, and economic instability will continue to grow. As well as threatening Western interests, China's dominance in the subsea cable industry could undermine numerous countries' economic and digital sovereignty, particularly in emerging markets. As such, the United States must take proactive measures, including harnessing the power of DFIs and facilitating international cooperation, to safeguard these cable networks and ensure a secure and resilient future for the world's communications infrastructure under the sea. This involves not only defending against physical threats but also protecting the integrity and reliability of the data transmitted through these cables. By prioritizing the protection of undersea infrastructure, the United States and its allies can mitigate the risks posed by adversaries and secure the digital backbone of the global economy. ■

***Daniel F. Runde** is a senior vice president, director of the Project on Prosperity and Development, and holds the William A. Schreyer Chair in Global Analysis at the Center for Strategic and International Studies (CSIS) in Washington, D.C. **Erin L. Murphy** is a senior fellow with the Asia Program at CSIS. **Thomas Bryja** is a research assistant and program coordinator with the Project on Prosperity and Development at CSIS.*

The authors would like to thank Emma Jing for her writing and research support.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax- exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2024 by the Center for Strategic and International Studies. All rights reserved.