FIU Jack D. Gordon Institute for Public Policy

Policy Innovation Series

April 2026

From the Caribbean to the Pacific coast of South America: Undersea Cables and China's Strategic Control of Information Flows

Juan Pablo Toro and Martin Brown

Executive Summary

Undersea fiber-optic cables carry approximately 99 percent of global communications and underpin trillions of dollars in daily financial transactions, yet they remain vulnerable due to their commercially driven design and limited security oversight. The People's Republic of China (PRC) has integrated these systems into its Digital Silk Road strategy, using firms such as HMN Tech to expand control over global telecommunications infrastructure and data flows. Moreover, China's legal framework, including its 2017 Cybersecurity Law, further enables state access to data managed by Chinese firms operating abroad. Overall, China's undersea cable expansion is not merely economic, but a form of infrastructure statecraft designed to generate persistent access, strategic dependency, and intelligence advantage.

In Latin America and the Caribbean, projects like the Suriname-Guyana Submarine Cable System demonstrate how reliance on Chinese maintenance and operational support can create long-term access to network infrastructure and data. When combined with surveillance systems such as Huawei smart cities, this produces a vertically integrated digital ecosystem capable of supporting intelligence collection and coercive leverage.

More notably, these dynamics extend to Pacific-facing states, where cable infrastructure, surveillance systems, and space-based assets reinforce multi-domain information control. For the United States, these developments risk creating asymmetric dependencies, including the Caribbean Basin, its "third border." Also, the United States should prioritize a coordinated regional response by expanding cybersecurity cooperation and infrastructure protection through CISA and the State Department's Bureau of Cyberspace and Digital Policy. It should also scale financing for trusted digital infrastructure alternatives through the U.S. International Development Finance Corporation to reduce reliance on Chinese providers. Finally, Washington should support partner nations in developing investment screening mechanisms modeled on CFIUS to strengthen oversight of foreign involvement in critical telecommunications infrastructure.

Introduction

Undersea fiber-optic cables make up 99 percent of global communications (civilian and military) and conduct daily financial transactions amounting to billions of dollars. Undersea cables are the backbone of modern communications, with more than 575 active cables, stretching over 870,000 miles across every ocean, effectively creating information superhighways. In 2023, undersea cables transmitted $10 trillion of financial transactions daily. Globally, the major players of undersea cables are Google, Meta, and Prysmian Group with steady expansions over the past few decades.

In addition, 98 percent of undersea cables are installed by a handful of firms, such as China's Huawei Marine Networks (HMN) Tech, represents more than 10 percent of all undersea cable projects. More notably, HMN was previously a subsidiary of Huawei, a Chinese firm sanctioned by the United States. Huawei's CEO, Ren Zhengfei, formerly served as an engineer in China's People's Liberation Army (PLA), a background often cited as indicative of the company's ties to the Chinese state. Due to U.S. sanctions and resulting supply chain pressures, driven by concerns that Huawei could potentially enable PLA-linked network interference, Huawei was compelled to sell HMN Tech. The company was subsequently acquired by Hengtong Optic-Electric Co., which took a 51 percent controlling stake. This acquisition allowed HMN Tech to avoid direct placement on the U.S. Department of Commerce's sanctions list, enabling it to continue investing in undersea cable projects globally.

Submarine digital infrastructure was not developed with maritime security in mind, but purely commercial criteria, especially at choke points. In its routing, cables often follow the same paths as sea lines of communication; hence their predictable routes. Presently, contemporary maritime environments face a combination of threats where geopolitical competition and confrontation among the great powers converge, the repercussions of regional conflicts, malicious actions by non-state actors, and environmental impact. These threats can be divided into five main categories: climate change, economic warfare, parallel fleet operations, damage to critical infrastructure, and illicit activities, ranging from illegal fishing to piracy.

Therefore, contemporary maritime security encompasses the protection of economic resources that exist on and under the surface, as well as the maritime infrastructures deployed along coasts, on the seabed, and in open waters. Protecting critical maritime infrastructure has become increasingly complex as these critical maritime infrastructures for navies and coast guards; at heart, it is a matter where connectivity and vital dependencies converge, especially when data is considered the "new oil" of the global economy.

China's Undersea Cable Strategy

The People's Republic of China's (PRC) strategy in undersea cable ownership stems from its Digital Silk Road (DSR). The DSR aims for the CCP to control 60 percent of the global submarine cable market. Additionally, DSR is the technological component to the PRC's Belt and Road Initiative, reflecting China's growing commitment to create a multi-dimensional form of infrastructure dependence in both the physical and technological domain. DSR is founded on two core ideas: interconnection of infrastructure across digital and physical domains. To achieve DSR goals, the PRC has been prominent throughout Latin America with surveillance infrastructure such as Ecuador's ECU 911 and Venezuela's Fatherland Card which achieve both interconnection and infrastructure dependency. On the physical side, the PRC creates data centers and telecommunications infrastructure, especially with the growth of undersea cables. In Latin America, undersea cables enable China to exercise dual-use capabilities to monitor, store, and understand information flows by civilians and military entities.

Moreover, China's push in Latin America through submarine cables has caused widespread concerns. Since 2017, China's Cybersecurity Law requires both companies and entities to report to the PRC's state intelligence services. As a result, the Chinese Communist Party's (CCP) integration of submarine cables creates vulnerabilities in the monitoring and storage of data traffic throughout the Western Hemisphere. Ultimately, submarine cables are highly vulnerable, with low barriers of disruption by both state and non-state actors despite their critical role in global communications. Measuring only 2 to 18 centimeters in diameter, they can be easily damaged through anchors or targeted sabotage such as explosives, as seen in the Baltic Sea, near Taiwan, and in the Red Sea. In addition, Western countries have claimed that China deliberately sabotages or wiretaps international submarine cables. Presently, malicious groups with Chinese origin may attempt to infiltrate the Western Hemisphere's critical infrastructure by opening access to undersea cables. Firstly, China's state-sponsored Salt Typhoon are known for carrying out espionage may focus on sabotaging fiber backbone infrastructure and data routing operations in undersea cables. Secondly, China's state-sponsored Volt Typhoon are known for launching malware against communication nodes and logistical facilities to gain access and enable potential disruption in future geopolitical escalation.

For the PRC, undersea cables are not just infrastructure but allow for a position of strategic control of transmission nodes. China's 2017 Cybersecurity Act integrates companies with state-sponsored intelligence operations to establish local storage, auditing, and data transfer requirements for critical infrastructure operations. This enables China to gather massive amounts of data across the globe for the purpose of monitoring for vulnerabilities in foreign powers. Submarine cables function as an extraterritorial tool of control by combining digital infrastructure with physical assets and diplomatic entanglement through the storage and potential manipulation of private data.

Additionally, the PRC's Global Initiative on Data Security pushes Beijing to grow in global cooperation for newer developments in maintaining supply chains for telecommunications to promote a digital economy and interconnectedness. Undersea cables act as a critical dual-use infrastructure for Beijing in Latin America. Currently the PRC has more than ten satellite bases in the Western Hemisphere including four Signal Intelligence (SIGINT) spy bases in Cuba and eleven satellite bases throughout Latin America. So, investing in undersea cables to coastal nations tied to these sites makes it imperative for the PRC to gain real-time information, gathered from these bases. Data Security is central to PRC operations to secure their data from dual-use infrastructure and surveillance in other foreign countries.

In total, Beijing's undersea cable strategy relies on HMN Tech to develop the digital economy that China seeks to grow from the DSR. By the end of 2024, Chinese enterprises have invested in 17 in-service international submarine cable systems. Of these projects, HMN Tech stands as one of the four major global engineers, procurement, and construction contracts for submarine cables, delivering over 100,000 km of undersea cable networks in more than 70 countries. HMN was previously owned by Huawei yet due to U.S. sanctions, Huawei sold HMN to China's Hengtong group. Hengtong is one of the largest power and fiber optic cable producers in the world with 70 subsidiaries. More notably, HMN Tech has many foreign cable project investments especially in Latin America, where they contain projects in the Caribbean, Peru, Bolivia and Chile.

Caribbean Nation's Undersea Cable Engagement

The Suriname-Guyana Submarine Cable System's (SG-SCS) main supplier is HMN Tech and has been in service since 2010. The cable is an estimated 1,249 km long and although owned by Guyana Telephone and Telegraph, they are heavily reliant on HMN for operation of the cable. The landing points for SG-SCS are Georgetown, Guyana, Totness, Suriname, and Chaguaramas, Trinidad and Tobago. HMN Tech has been responsible for maintenance and support for the upkeep of the project. Throughout its role as the primary maintenance provider, HMN prioritized customer service and transmission of software updates/integration.

This project allows over 500,000 people in Suriname to access the internet with local network bandwidth increasing by over 3,000 times. Also, HMN aims to develop both an Equipment Health Check and Network Evaluation Optimization, allowing the PRC to monitor and manage both hardware and software systems. This persistent involvement by the PRC as the manager of SG-SCS creates ongoing control for privileged, long-term access to both the physical and digital infrastructure amongst all forms of communication (civilian and military). This allows PRC intelligence operations to conduct data interception and metadata collection due to limited cybersecurity oversight by host nations in the Caribbean.

Furthermore, control of these critical juncture points could allow opportunities for the PRC to disrupt or delay communications services in times of extreme political tension, acting as economic and military pressure points. Beijing's ownership signals an asymmetric dependency in which technical reliance transfers into strategic influence. Also, the landing points of Georgetown, Totness, and Chaguaramas have growing importance in the Caribbean. For example, the growth of ExxonMobile offshore oil production in Guyana as in late 2025, daily oil production hit 900,000 barrels a day. By 2030, Exxon aims to ramp up oil production to 1.7 million barrels a day. Yet, this plan of future energy investments may be undermined due to the PRC's ability to monitor communication lines through cyber espionage such as wiretapping, allowing them to precisely invest in areas vulnerable or ignored by Exxon in Guyana's oil industry.

In 2019, Huawei installed 100 smart cameras, valuing more than $35 million with facial and vehicle recognition systems across Georgetown, Guyana. This project includes a security control room, having access to the real-time monitoring of the city's surveillance, granting Huawei unprecedented access to monitor Guyana's civilian and military sectors. Huawei's surveillance data is often collected and stored in their data centers in China requiring secure and rigorous transmission networks to aid in this processing, potentially with HMN Tech acting as the backbone of transmission of cross-border analytics and cloud processing through their undersea cables. This structure introduces risks related to data access, system

manipulation, and dependency, enabling potential intelligence collection and coercive leverage during periods of geopolitical tension.

SG-SCS presents a significant geopolitical risk for the United States. For the U.S., the Caribbean serves as the "third border" both economically and militarily. Yet, the real-time monitoring produced by Huawei's surveillance capacities grants significant opportunities to undermine strategic autonomy of Caribbean nations like Guyana but also U.S. investments in the region as well. Undersea cables can enable network mapping and traffic analysis, potentially tracking U.S. maritime vessel movements through monitoring communication lines.

Beijing's Investments in Pacific Facing Nations

The Caribbean is not the only focus for China in undersea cable management but also the Andean region and Pacific facing nations. This is most specifically due to China's growing economic and military presence in nations such as Peru and Chile. For example, the Fibra Optica al Pacifico (FOP) supplied by HMN Tech spans more than 1,200 km along Peru and into Bolivia. FOP was ready for service September 2020, and it is owned by Entel Bolivia to support telecommunications, internet access, and enterprise connectivity.

Although in Peruvian waters, FOP was created by the Bolivian government to increase internet speed while lowering costs for the civilians. The undersea cable begins in the Port of Ilu to Lurin in Peru with an additional ring of Tacna, Tarata, Mazocruz, Huaytire, Moquegua, and Mollenda on the borders between Peru and Bolivia. The total investment ranges between $40 to $60 million. For Beijing, this allows for access to Peru, Bolivia, Chile, and any other neighboring Latin American nation's communication lines. More significantly, Lurin is an estimated 40 km from Lima, Peru's capital which potentially monitors communication from Peru's most populated city. In the Callao province, bordering Lima and an estimated 45 km away from Lurin, China's Dahua invested a hundred cameras throughout the province to monitor traffic with speed domes.

This investment by Dahua also requires transmission devices through a wireless solution. When paired with the undersea cables, this arrangement produces a vertically integrated digital architecture spanning data collection, transmission, and analysis. The ownership of the cable remains with Entel Bolivia but operational control is externalized to the PRC for equipment, maintenance, and system optimization, creating sovereignty dependence. This dependence creates critical opportunities for the CCP to collect and document the movement of civilian and military entities throughout Bolivia and Peru. Moreover, this undersea cable is strategically close to China's Amachuma space facility in Bolivia.

The Amachuma space station was inaugurated in 2013 and operated by China's Great Wall Industry Corporation to track TKSAT-1 which is a payload satellite conducting an operational mission focused on civil communication. This satellite was launched at the Xichang Space Center in China under the Chang Zheng 3B launch vehicle which was built by the China Association for Science and Technology. FOP and the Amachuma are a part of the same information ecosystem and rely on each other to move information in real time to Beijing. The FOP enables the transmission of vast quantities of data, space- and ground-based satellite systems provide additional layers of monitoring, redundancy, and intelligence collection. These capabilities create multi-domain leverage that link PRC operating seabed infrastructure to terrestrial networks, and space-based assets. This allows China to observe, map, and potentially influence key components of Bolivia and Peru's digital infrastructure. However, not all projects by the CCP succeed in engaging with Latin America. Presently many steps are being taken by newly elected governments throughout Latin America to impede PRC presence in the region, especially in dual-use technology.

An underwater fiber-optic cable project aiming to connect Chile and China sparked controversy when the U.S. State Department announced in February 2026 that it was revoking the visas of three government officials of President Gabriel Boric's administration (2022–2026), without identifying them (the minister of Transport and Telecommunications, Juan Carlos Muñoz; the undersecretary of Telecommunications and other officials in that ministry), stating that they "directed, authorized, funded, provided significant support to,

and/or carried out activities that compromised critical telecommunications infrastructure and undermined regional security in our hemisphere". The cable, 19,873 kilometers long, which would stretch between the cities of Concón and Hong Kong with 266 repeater stations in international waters and 16 in territorial waters, was promoted by China Mobile International, which was seeking to invest $500 million.

The controversy deepened even more over the contradictory accounts from Boric administration officials. While some argued that it was merely a project under study, a major local newspaper published a decree dated January 27, 2026 that reported its approval; the same decree was annulled just two days later for a "technical or typographical error." The Embassy of the People's Republic of China rejected the American maneuver concerning a cable that would strengthen "Chile's communications with its largest trading partner" and would help consolidate this South American country's regional leadership "in the digital economy and communications networks".

At a press conference, the American ambassador to Chile, Brandon Judd, without identifying the names of the actors involved, argued that his government had warned Chile about incursions into Chile's telecommunications systems by foreign malicious actors, and referenced the case of a local company that was hacked amid a contest for future contracts. His warning was that when a country does not protect its critical infrastructure, it risks losing its sovereignty.

China's insistence on the cable, as part of the ongoing strategic dispute with the United States, undoubtedly goes beyond the desire to connect with Chile, one of its many regional partners. Possible explanations include: seeking autonomy from Trans-Pacific cables, whose monopoly today belongs to the United States; using the South American country as a platform to access third-country data markets, such as Brazil; or betting on future networks that would allow connectivity with Antarctica, these are hypotheses that have emerged behind the marked interest of the Chinese company. As if that weren't enough, the controversy occurred when the Chilean government had already awarded the construction of a submarine cable to the American company Google to connect the country to Asia via Australia.

The Chilean government's decision to route the Humboldt Cable via Australia, rather than establishing a direct link to a Chinese city, reflected a technical and strategic assessment. As noted in the concession award report from the Undersecretariat of Telecommunications, this infrastructure will position Chile as a regional digital hub, prioritizing data security and network redundancy. This choice also aligned with prior analyses by the Ministry of Transport and Telecommunications, which had warned about the urgency of diversifying Trans-Pacific cables to avoid technological dependencies and disruptions, a critical factor in the context of the current US–China technology rivalry.

The conservative president José Antonio Kast, who took office on March 11, 2026, announced that he would first wait for the Humboldt Cable to become operational by the end of next year before making any decision about the Chinese project. However, his alignment with the United States, ratified through his participation in the "Shield of the Americas" summit on March 7, along with other gestures and statements favorable to actions of the Donald J. Trump administration in Venezuela and Iran, makes it unlikely that the Chinese project will come to fruition during his four-year term.

For Chile, the underlying problem is that it lacks legal frameworks or institutions that would allow evaluating the national security consequences that certain critical infrastructures may pose to itself and to its partners. On the one hand, it appears to yield to the persistent pressure from the United States, its main security partner, and on the other hand, it alienates China, its main trading partner, paying a high diplomatic cost for lacking the tools to decide which technology to allow within its territory.

Policy Recommendation

The protection of maritime infrastructure must gain greater attention by all nations in the Western Hemisphere The United States and nations in the Western Hemisphere have significant opportunities for the growth and security of their data and communication networks within the maritime domain.

Firstly, creating undersea cable resilience is key in the operation and manufacturing of undersea cables. The United States' Cybersecurity and Infrastructure Security Agency (CISA) should prioritize working with our partner nations in the Western Hemisphere to aid in the regulation and implementation of telecommunications. This should be also conducted through the U.S. State Department's Bureau of Cyberspace and Digital Policy (CDP) in partnership with Organization of American States (OAS). CISA can aid in elevating the undersea cable security through training fundamentals on vulnerabilities that may appear with maritime infrastructure. These trainings can also include landing-station cyber hygiene assessments, incident response exercises, and access-control standards for foreign vendors.

Secondly, the CDP focuses on both digital connectivity and cybersecurity partnership with the focus on promoting open, interoperable, reliable, and secure internet for the purpose of telecommunication asset protection. Moreover, every embassy in a country with major landing points should maintain a digital infrastructure risk dialogue with the host government to produce a confidential vendor-risk matrix and procurement standards requiring local data collection.

Thirdly, through the maritime component of U.S. Southern Command (SOUTHCOM), initiatives can be promoted to work with regional partners to improve collective Maritime Domain Awareness (MDA). The MDA, defined by the International Maritime Organization as the effective understanding of anything associated with the maritime domain that could impact security, safety, the economy, or the environment, not only encompasses what happens on the surface of the seas and above it as traditionally believed, but also what lies beneath it, including critical infrastructure such as fiber-optic cables. Its surveillance and protection are crucial for the economies of the Western Hemisphere. In order to create or improve the Underwater Domain Awareness (UDA) or Subsurface Awareness, as a distinct but integrated component of MDA, new technologies can be integrated, as unmanned underwater vehicles, or cable protection can be included as part of combined naval exercises too.

Fourth, the U.S. International Development Finance Corporation (DFC) should aid private and public corporations in co-financing and providing incentives for maritime infrastructure in Latin America and the Caribbean for backing digital infrastructure. These priority windows are for trusted digital infrastructure in the Caribbean and Pacific coast of South America through cable landing station modernization and redundant backhaul routes. Finally, the U.S. should work in sharing the frameworks and legal background of the Committee of Foreign Investment in the United States (CFIUS). CFIUS is the United States' way of protecting from invasive foreign actors from investing in critical infrastructure. Sharing the process of this initiative to allies in the Western Hemisphere may allow them to gain a greater strategic autonomy when considering foreign investments from malicious actors like China. The U.S. Department of State, Commerce, and Justice should send representatives to each Latin American nations to aid in the implementation and creation of their own respective oversight mechanism in order to counter and monitor foreign engagement. It is imperative that each Latin American nation is given their own right to choose and have the strategic autonomy to grow their nation without foreign actors influencing their policies. This can be done most actively through national oversight mechanisms that work to mitigate and respond to growing threats in critical infrastructure.

Conclusion

Finally, in the Western Hemisphere, undersea fiber-optic cables have emerged as one of the most consequential yet vulnerable components of modern geopolitical competition. As the backbone of global communications and financial systems, their security is no longer a purely technical or commercial concern, but a strategic imperative. The expansion of the PRC's presence in submarine cable infrastructure, particularly through firms such as HMN Tech, reflects a broader effort to embed itself within the global digital ecosystem and shape the flow of information across regions critical to U.S. interests.

In Latin America and the Caribbean, these dynamics are already visible. Projects such as the Suriname-Guyana Submarine Cable System, alongside integrated surveillance architectures, demonstrate how infrastructure ownership and operational

control can translate into persistent access, data exposure, and long-term dependency. In Pacific-facing states, similar patterns emerge through the convergence of cable systems, terrestrial networks, and space-based assets, creating multi-domain information environments that enhance the PRC's capacity for monitoring and influence.

For the United States, these developments carry direct implications for regional stability and its own strategic posture, particularly within the Caribbean as a "third border." The risk is not limited to disruption, but extends to intelligence collection, economic leverage, and the gradual erosion of partner nations' strategic autonomy. Addressing this challenge requires a shift from reactive measures to proactive engagement. Strengthening infrastructure security, supporting regulatory capacity, and providing credible alternatives to foreign-controlled systems will be essential. Ultimately, maintaining a secure and resilient digital environment in the Western Hemisphere will depend on sustained coordination, investment, and strategic alignment between the United States and its regional partners.

Authors

Juan Pablo Toro is a Senior Research Fellow at AthenaLab think tank (Chile) and Senior Associated Fellow at RUSI. He is also an adjunct assistant professor at the Faculty of Communications of the Catholic University of Chile and a columnist for the newspaper El Mercurio. He writes articles for specialized publications and book chapters on geopolitics of the Americas, the Indo-Pacific, and Antarctica.

Martin Brown is a graduate student in Global Affairs at Florida International University and a research analyst at the Jack D. Gordon Institute for Public Policy, where his work focuses on China's global strategy, security engagement, and intelligence activities, with a regional emphasis on Latin America and the Caribbean. He has supported analytical efforts for U.S. Southern Command and the National Geospatial-Intelligence Agency, integrating OSINT and GEOINT methodologies to examine dual-use infrastructure, surveillance technologies, and non-traditional security cooperation. His research has been published in outlets including *The Diplomat*, *Americas Quarterly*, and *Infobae*, and centers on how China operationalizes strategic influence across regions, contributing to broader debates on great power competition and global security.

Disclaimer