JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(2), 568-579
ISSN: 2589-1316

Undersea Cables in the South China Sea: A New Frontier of Us-China Strategic Competition and The Dilemma for Southeast Asian Countries

Nguyen Hung Vuong [1]*, Vo Ha Chi[2]

[1] *University of Foreign Language Studies, The University of Danang, https://orcid.org/0000-0003-1534-2778*
[2] *University of Foreign Language Studies, The University of Danang*

*__Corresponding Author:__ philosophy.hv.ud@gmail.com

Citation: Vuong, N. and Chi, H. V. (2025). Undersea Cables in the South China Sea: A New Frontier of Us-China Strategic Competition and The Dilemma for Southeast Asian Countries, *Journal of Cultural Analysis and Social Change*, 10(2), 568-579. https://doi.org/10.64753/jcasc.v10i2.1640

Published: November 12, 2025

ABSTRACT

This research paper examines the strategic competition between the United States and China over undersea fiber-optic infrastructure in the South China Sea, a region rapidly emerging as a new frontier in the global digital order. Drawing on the theory of "Weaponized Interdependence", the article demonstrates how these undersea cables have become politicized, serving as instruments for exerting systemic influence, enacting strategic denial, and applying soft coercion. While the US promotes undersea cable networks designed to bypass China and thereby secure global data chokepoints, China is concurrently making significant investments in digital infrastructure through its "Digital Silk Road" initiative. This intensifying contest beneath the South China Sea heightens the risks of infrastructure disruption, infringes upon digital sovereignty, and places Southeast Asian nations in a complex strategic predicament. The paper argues that ASEAN countries must move beyond a passive stance to actively assert their strategic role. This involves forging a "collective digital sovereignty" characterized by common technical standards, independent data centers, and collaborative measures to protect digital infrastructure security. Such an approach aims to prevent ASEAN nations from being drawn into the technological orbits of the superpowers, thereby safeguarding their centrality within the regional security order.

Keywords: Undersea fiber-optic cables; South China Sea; US-China competition; Digital power; Digital Sovereignty

INTRODUCTION

Recent years have witnessed profound geopolitical, security, and economic crises, fueling a continuous escalation of strategic competition among major powers. Tensions between the US and China have significantly expanded, transcending traditional trade and geopolitical rivalries to encompass the realm of information and communication technology (ICT) infrastructure, particularly within deep-sea fiber-optic cable systems (Zheng, 2024; Scobell, 2018). This marks a crucial shift in the nature of competition between the two superpowers, from military security threats and trade tariffs to vying for control of "strategic nodes" within the global digital infrastructure network (Farrell & Newman, 2019, pp. 44-45). As critical infrastructure for global communication networks, undersea cables are emerging as a "new front" in the US-China strategic competition. These cables currently carry over 97% of international data traffic (Geri, 2023), implying that dominion over them equates to control over global information flows. Against this backdrop, the US and China are relentlessly advancing their strategies to control and protect undersea cables, seeking to maintain or augment their strategic power and

influence. Through companies like Google, Meta, and SubCom, the US has been heavily investing in trans-Pacific and trans-Atlantic undersea cable projects, not only for economic benefits but also to preserve political influence regionally and globally. Conversely, with its "Digital Belt and Road" strategy, China has increased the construction of undersea cables connecting Asia with other regions, while simultaneously aiming to reduce reliance on Western-controlled cables (Freedman, 2021; Zheng, 2024). The South China Sea, a conduit for numerous vital undersea cables, has become an indispensable part of this US-China arena for control over cable infrastructure. Competition over undersea cables in this region could lead to changes in the cable system and the balance of power among regional states. Some Southeast Asian countries stand to become hubs for new trans-Pacific networks, while others risk being marginalized, unable to connect to crucial undersea cable systems.

In recent years, the US-China undersea cable competition has attracted increasing scholarly attention in the region. However, these studies predominantly focus on cybersecurity aspects and information security issues, lacking in-depth analysis of the competition's impact on Southeast Asian security and the strategic decisions of Southeast Asian nations in selecting telecommunication infrastructure partners. Furthermore, current research, such as Zhang (2024), Zheng (2024), and Zhang & Hou (2024), primarily highlights the competitive relationship between the major powers without adequately analyzing the predicament facing Southeast Asian nations, often compelled to choose sides between the two superpowers. Countries like Vietnam, the Philippines, and Malaysia not only face pressure from the US and China in selecting cable partners but also have to contend with rising cybersecurity risks as cables transiting the South China Sea may become potential targets for sabotage or espionage. This research employs a qualitative analysis of official documents, strategic reports, and case studies on Southeast Asian countries, alongside a comparative method to contrast US and Chinese strategies. Accordingly, this study seeks to address two pivotal research questions: (i) How will the US-China undersea cable rivalry in the South China Sea impact regional security in Southeast Asia? and (ii) How will regional countries respond—by cooperating, choosing sides, or pursuing other avenues? Therefore, investigating the impact of the US-China undersea cable competition in the South China Sea is not only significant for global cybersecurity but also crucial for informing the security development strategies of Southeast Asian nations.

Undersea Cables: A New Frontier in Great Power Infrastructure Competition

In the global digital ecosystem, undersea fiber optic cable systems have become the backbone of the international Internet, carrying the vast majority of cross-border data traffic. It is estimated that 95% to 99% of international data, including financial, communication, military, commercial, and personal information, is transmitted via undersea cables, rather than via satellites, as is commonly perceived (Runde, 2023; Noor, 2024). With transmission speeds reaching terabits per second and superior stability, undersea cables are the sole means capable of meeting the immense demand for instantaneous and continuous connectivity in the modern digital economy. This system not only serves a purely technical function but has also become a strategic infrastructure pillar for nations and international organizations. Cannon (2024) emphasizes that modern undersea cables do more than connect geographical points; they also link data centers, cloud computing platforms, and global AI infrastructure, thereby determining the operational capacity of the digital economy. The rapid development of technologies such as artificial intelligence (AI), Big Data, the Internet of Things (IoT), and streaming video services has increased pressure on existing undersea cable systems, demanding continuous expansion in scale, speed, and connectivity range (Capri, 2024).

From a geopolitical perspective, undersea cables are understood as power infrastructure, as control over cables equates to control over data – an increasingly central factor in policymaking, economic operations, and modern military campaigns. Farrell and Newman (2019) term this phenomenon "Weaponized Interdependence". Accordingly, nations controlling data networks can use that access as a tool for coercion, punishment, or surveillance of adversaries without overt military intervention. The power shift from physical space to data space renders undersea cables strategic assets and "dual-use assets" in national security strategy – serving both commerce and surveillance/counter-espionage. Indeed, some nations now regard undersea cables as critical infrastructure requiring protection akin to that afforded to power plants, airports, or arsenals (Noor, 2024). The sabotage or damage of undersea cables, whether accidental or intentional, can severely impact global trade, central bank operations, defense system functionality, and emergency coordination during disasters. As of 2024, there are over 486 active submarine fiber optic cables worldwide, with a total length exceeding 1.4 million km, largely concentrated in strategic areas such as the North Atlantic, the South China Sea, the Indian Ocean, and the Pacific region (Capri, 2024). This is the physical realm where the global power structure in the digital age is being constructed and contested, millimeter by millimeter.

Historically, political power has been intrinsically linked to the control of physical space: territory, territorial waters, or airspace. However, in the 21st century, the realm of power has expanded decisively into the digital domain, where transnational data networks become instruments for shaping influence and exercising soft power.

Undersea fiber optic infrastructure, initially considered auxiliary technical structures, has now become a tool for structuring geopolitical power, especially amidst the escalating strategic competition between the United States and China. According to the theory of "Weaponized Interdependence", in a world densely interconnected by global networks spanning finance, logistics, the internet, and information, nations controlling strategic nodes within these networks can exert pressure, monitor, or disrupt information flows and transactions, thereby reshaping the global order to their advantage. In the case of undersea cable infrastructure, transit hubs, installation and operating companies, and transnational data centers form the "strategic nodes" that can be weaponized under the guise of national security or coercive diplomacy (Farrell & Newman, 2019, pp. 44–47).

The US has long recognized the strategic role of undersea cable infrastructure as an extension of soft power in the digital age. American technology companies like Google, Meta (Facebook), Microsoft, and Amazon are not only consumers of international bandwidth but also owners or investors in dozens of transoceanic cables such as Dunant, Equiano, Curie, Apricot, or Echo (Capri, 2024, pp. 7–10). Washington, under both the Trump 1.0 and Biden administrations, has actively implemented technology and digital security policies, preventing Chinese companies like HMN Technologies (formerly Huawei Marine Networks) from participating in international cable projects such as SeaMeWe-6 or the Pacific Light Cable Network (Runde, 2023; Noor, 2024). China's exclusion from the SeaMeWe-6 project was not merely a commercial decision but a clear indication of strategic competition in the digital space. Conversely, China is advancing its "Digital Silk Road" strategy, with the parallel objectives of exporting telecommunications infrastructure and establishing independent undersea cables connecting China to partners in the Middle East, Africa, and Europe through routes like the PEACE Cable (Pakistan & East Africa Connecting Europe) and AAE-1 (Asia Africa Europe-1). Companies such as Hengtong Marine, China Telecom Global, China Mobile, and particularly HMN Tech have become key instruments for implementing an industrial policy that integrates military and civilian objectives (CSIS, 2023).

The US-China confrontation in undersea cables extends beyond investment competition to concerns about "soft security", especially amid growing accusations of sabotage, espionage, or attacks on subsea digital infrastructure. A report by McCartney (2024) indicated that the US and its European allies have intensified surveillance of Chinese cable ships due to concerns about potential "cable cutting", installation of signal interception devices, or electromagnetic signal harvesting from cable systems. Baraniuk (2023) also confirmed that modern cables can be tapped, disrupted, or sabotaged by sophisticated digital and physical means, particularly at landing stations, widely considered the most critical security vulnerabilities in the global cable system. In this strategic "gray zone" – where there is no clear declaration of war, yet all actions can be weaponized – undersea cables become a "new geopolitical boundary", allowing superpowers to manipulate data flows and exert influence without territorial occupation. It is this blurring between civilian infrastructure and military strategy that makes the undersea cable system one of the most vulnerable yet least attended to areas in modern international security.

In the era of modern geostrategic competition, each undersea cable symbolizes a nation's or an alliance's capacity to project international influence. The investment structure, geographical routing, and technical presence of these cables have gradually shaped invisible boundaries where political influence is "transmitted" in parallel with data flows. Consequently, in recent years, China has vigorously pursued its "Digital Silk Road" strategy through large-scale undersea cable projects aimed at reducing dependence on routes transiting Western territories or involving Western companies. A prominent example is the PEACE Cable (Pakistan & East Africa Connecting Europe), over 15,000 km long, connecting China with Pakistan, Djibouti, Kenya, Egypt, and Europe, functioning as a data corridor parallel to US-controlled routes (Capri, 2024; Cannon, 2024). The PEACE Cable not only connects telecommunication infrastructure but is also accompanied by investments in seaports, data centers, and technology platforms from Chinese companies such as Hengtong, Huawei Marine Networks (now known as HMN Technologies), and China Telecom Global. Besides PEACE, China has backed projects like Asia-Africa-Europe-1 (AAE-1) – a cable running from Hong Kong to France, traversing strategic regions like the South China Sea, Indian Ocean, and the Middle East. Additionally, the Silk Road Fiber Cable, a transcontinental cable connecting China to Europe via Central Asia and Turkey, is seen as an overland extension of the cybersecurity strategy integral to The Belt and Road Initiative (BRI) (Noor, 2024).

In this context, the United States, along with key technology corporations like Google, Meta, Amazon, NTT (Japan), and Singtel (Singapore), has implemented a series of systematic strategic responses. Instead of sharing or competing within existing routes, Washington and its allies have accelerated the construction of an "independent cable belt" network. This network comprises cables that do not transit through China-controlled areas, thereby aiming to ensure data transmission autonomy and mitigate cybersecurity risks. Cables like Apricot, connecting Japan, Taiwan, the Philippines, Guam, Indonesia, and Singapore, are designed to "completely bypass" mainland Chinese infrastructure. Similarly, the Echo cable will, for the first time, directly connect Singapore to the US via Indonesia, while Bifrost creates a secure data corridor from Singapore to Guam and the United States, funded by the US and its regional allies. Previously, SEA-US commissioned a cable connecting the Philippines–Guam–Hawaii–California, demonstrating effective coordination between Southeast Asian carriers and US partners.

Notably, the exclusion of HMN Technologies from the SEA-ME-WE 6 project in 2022 due to direct US pressure clearly shows Washington's decisiveness in halting Beijing's infrastructure influence. The investment structure in these cables is not merely an economic calculation but reflects a long-term geopolitical strategy to establish US-controlled data corridors, ensuring resilience in digital crises and deterring infrastructure interference from strategic rivals like China (Brock, 2023; Capri, 2024).

Situated at the crossroads of East Asia, Southeast Asia, and the Indian Ocean, the South China Sea is not only a global maritime lifeline but also an increasingly critical digital chokepoint in the global information infrastructure network. According to Telegeography data (2024), the South China Sea region currently hosts over 20 international submarine fiber optic cables that transit or land in coastal nations such as Vietnam, the Philippines, Singapore, Malaysia, and Brunei, directly connecting Northeast Asia with South Asia, the Middle East, Europe, and North America. Cables like the Asia-America Gateway (AAG), SEA-ME-WE 3, Intra-Asia (IA), or Asia Direct Cable (ADC) are not only economically significant but also constitute strategic transnational infrastructure serving e-commerce, communications, state governance, and digital defense activities. In this context, each cable becomes a hidden power boundary beneath the South China Sea, where the nation controlling investment, installation, and maintenance rights gains a strategic advantage in managing data flows, tantamount to controlling global information supply chains. Southeast Asian nations are no longer mere recipients of infrastructure but are becoming intermediate pivots in the reshaping of the digital geopolitical map between the US and China. The choice of investors, routing, and maintenance entities is no longer a technical issue but profoundly political; each choice can become a strategic positioning maneuver, fraught with the risk of being drawn into the sphere of influence of one of the two superpowers.

More alarmingly, the South China Sea is also where China is incrementally expanding "soft control" through the administrative instrumentalization of infrastructure. Beijing's delay or refusal to grant seabed survey permits for cable projects not under its control (Tan, 2024), or its demand for Chinese companies to undertake repairs in disputed areas, indicates a trend of weaponizing civilian infrastructure to reinforce sovereignty claims. In such a scenario, cables are not just tools for connectivity but also digital markers on a disputed sovereignty map, where political power is wielded through fiber optics rather than military force.

Power Projection: The US-China Strategic Clash in Undersea Cables in the South China Sea

As the world transitions from a traditional geopolitical order to a more fragmented digital one, undersea fiber-optic cables have become essential tools for great powers to project systemic influence. The US-China confrontation is not merely a contest for infrastructure control but, more profoundly, a competition to shape the global network order, where undersea cables serve as the "foundational architecture" in this new power space. According to Farrell & Newman (2019), in a world interconnected by global undersea cable networks, nations controlling "nodes" and "chokepoints" can shape international behavior through structural power – the ability to set the rules of the game rather than merely abiding by them. In the case of undersea cable infrastructure, the US and China are employing this very model to establish influence in transnational digital space, particularly in strategic regions like the South China Sea and Southeast Asia.

The US is forging a digital infrastructure ecosystem "selectively decoupled" from China to maintain its digital supremacy and protect long-term cybersecurity. The formation of cables like Echo, Apricot, and Bifrost, all avoiding territories or landing points potentially controlled by China, demonstrates the effort to establish a trusted connectivity network controlled by the US and its allied companies (Capri, 2024; Runde, 2023). Furthermore, the policy prohibiting US companies from using infrastructure linked to Hong Kong or HMN Technologies shows that Washington views undersea cables as a soft national security front, where technical standards are intertwined with power strategy. Meanwhile, China harbors ambitions of creating a parallel infrastructure order via its "Digital Silk Road", employing strategy integrating undersea cable investment, data center construction, 5G standard development, and cloud computing space control. China-backed cables like PEACE Cable or AAE-1 not only aim to expand connectivity but also serve to establish distinct infrastructure corridors, linking developing partners to China's technological ecosystem (Cannon, 2024; Noor, 2024). China not only installs infrastructure but also actively proposes encryption standards, provides surveillance technology, and offers credit support to recipient nations, thereby projecting soft power in the global digital space.

In the South China Sea, the parallel presence of US and Chinese cables is not just a manifestation of an infrastructure race but a clash between two paradigms of digital order: one oriented towards openness, standardization, and security; the other towards integration, control, and regionalization. The intervention of the two superpowers in the construction, maintenance, and licensing of cables in these waters is evidence that undersea cables have transcended their technical role to become a new physical frontier for influence strategies. While most strategic analyses of the South China Sea focus on the militarization of artificial islands or disruptive actions

challenging sovereignty, a new layer of power is silently forming beneath the waves, where undersea cables become tools for long-term, non-military influence projection by both the US and China.

In this region, both superpowers are vigorously pursuing a strategy of "digital flag-planting" by establishing networks of cables connecting Southeast Asia. According to Capri (2024), Vietnam, the Philippines, Singapore, and Malaysia boast the highest density of landing points in the region, where over 20 international cables converge, including critical ones like AAG, SEA-ME-WE 3, Intra-Asia, SEA-US, and Asia Direct Cable (ADC). Control over landing infrastructure in these countries is strategically as significant as controlling straits or forward island chains. The United States and its tech companies have deployed numerous cables that bypass disputed waters, concurrently directing landings towards strategically aligned nations. The Echo and Apricot cables, sponsored by Google and Meta, transiting Singapore, Indonesia, the Philippines, and Japan, are structured to completely avoid territory or waters claimed by China. Landing points are selected at stable digital transit hubs like Tuas and Changi (Singapore) and Batangas (Philippines), where the US has deep defense ties and a regular military presence (Runde, 2023). Concurrently, projects like Bifrost (2024), developed by Facebook and Keppel T&T (Singapore), not only aim to increase bandwidth but also reflect a strategic intent to open a secure data corridor from Southeast Asia to the United States, via reliable transit points such as Guam and Palau (Capri, 2024).

Conversely, China is pursuing a strategy of "soft encirclement" by promoting cables that transit through countries receptive to infrastructure investment, while integrating these routes with maritime spaces Beijing unlawfully controls. Cables like the PEACE Cable, connecting Gwadar (Pakistan) to Mombasa (Kenya) and Marseille (France), are designed with subsidiary branches passing Hainan Island and aiming for subsea connections into the South China Sea, thereby consolidating China's position as a "super-hub" for mainland Asian cables. Not content with controlling existing cables, China also implements an administrative mechanism of influence by delaying seabed survey permits, requiring investors to use Chinese contractors, or compelling route adjustments to avoid "sensitive" areas (Tan, 2024). These actions not only create disguised technical barriers but also reinforce sovereignty claims through a "submerged" presence in infrastructure operation. Each denial of a survey permit by China represents a step towards "not declaring sovereignty but compelling recognition of de facto control".

This situation places Southeast Asian nations in a position of having to choose between cable providers – a seemingly technical choice with profound geopolitical consequences. Landing a cable with China may come with technical support and low costs but carries risks regarding data security and loss of digital sovereignty. Conversely, landing cables backed by the US demands transparency and adherence to high standards but may provoke a reaction from Beijing. This is a mechanism of projecting influence on the ground via subsea infrastructure, where undersea cables are no longer neutral objects but have become strategic encodings of a digital order being shaped beneath the South China Sea.

China is a leading nation in combining telecommunications infrastructure with a strategy of exporting its digital development model. Through the Digital Silk Road initiative – a branch of the BRI – China not only finances or invests in undersea cables like PEACE or AAE-1 but also provides accompanying credit support, experts, equipment, and technical training to recipient countries. In Cambodia, Pakistan, Myanmar, Sri Lanka, and Djibouti, cable installation is often accompanied by surveillance systems, data centers, and cloud storage platforms operated by Chinese companies. HMN Technologies, Hengtong, and China Telecom Global serve as prominent examples (Capri, 2024; Noor, 2024).This strategy creates a form of soft technical dependence, where recipient nations not only use Chinese equipment and standards but also become more deeply reliant on Beijing's technological ecosystem. Notably, some recipient countries lack the domestic capacity to operate and maintain these systems independently, forcing them to sign long-term maintenance contracts or cede technical management to the provider – a form of soft control disguised as cooperation. Researchers have warned that this is a form of structured influence-building, where China, without a military presence, can still access, control, or even exploit strategic information (Cannon, 2024; CSIS, 2023).

In this context, the United States approaches digital soft power by building reliable and voluntary networks. Instead of applying a comprehensive support model like China, Washington promotes initiatives such as Build Back Better World (B3W), the Partnership for Global Infrastructure and Investment (PGII), and blended finance mechanisms through USAID, OPIC, and IFC to assist developing countries in building high-quality, sustainable, and transparent digital infrastructure (Runde, 2023). Companies like Google, Meta, and Amazon typically invest in cables through joint ventures with local carriers, ensuring host nations share ownership, operational rights, and technical data. However, US soft power also creates another form of dependence: reliance on high security standards, complex legal regulations, and global cloud computing infrastructure controlled by American corporations. Although transparent and compliant with regulations, recipient nations still face the risk of being unable to build an independent digital ecosystem due to a lack of capacity.

In the South China Sea and Southeast Asia, these two models of digital soft power are intertwining and directly clashing. One side offers fast, low-cost, easily accessible infrastructure but with associated control risks; the other builds reliable networks but requires adherence to standards and faces higher costs, as well as political risks from

Beijing. In reality, many countries have adopted a hybrid strategy, cooperating with both sides to optimize benefits, but this also increasingly draws them into a soft polarization in the digital space, where every technical choice carries strategic consequences.

As undersea fiber optic networks become the lifelines of global data transmission, controlling or interfering with these cables not only yields a technical advantage but also creates a strategic coercive capability that can serve as a substitute for sanctions, diplomatic pressure, or military intervention. In the case of the US and China, undersea cables are gradually becoming a tool of soft veto, allowing the two superpowers to modulate behavior, neutralize the opponent's influence, and restructure regional connectivity networks in favor of their respective strategies.

In practice, the United States has repeatedly used its veto power in undersea cable projects to prevent China's strategic presence in global infrastructure systems. The most prominent incident was preventing HMN Technologies (formerly Huawei Marine) from participating in the $500 million SEA-ME-WE 6 project connecting Southeast Asia, the Middle East, and Europe. Although HMN initially won the installation bid, Washington pressured partners in the investment consortium to cancel the contract and replace HMN with SubCom, citing espionage and national security concerns (Brock, 2023; Noor, 2024). This is a clear example of using financial and political influence to exclude a rival from core connectivity networks to prevent potential signal intelligence gathering or data exploitation by a rival. Another example is the US refusal to grant an operating license for the Pacific Light Cable Network (PLCN), a joint project by Google, Meta, and China Soft Power, intended to directly connect Los Angeles to Hong Kong. Although cable construction was completed, the US government suspended the Hong Kong connection in 2020, citing concerns that China could monitor strategic information from data centers located in the special administrative region. Consequently, PLCN operates on a limited basis, connecting Google to the Philippines and Meta to Taiwan (Capri, 2024). This event demonstrates that even installed cables can be legally and administratively vetoed within the transnational data space.

Conversely, China also employs administrative, technical, and legal measures to delay or neutralize cables not under its control, particularly in the South China Sea region. In 2023, a cable project connecting the Philippines and Taiwan was delayed because Beijing refused to grant seabed survey permits in a disputed area, forcing investors to reroute the cable, thereby extending timelines and increasing deployment costs (Tan, 2023). This is a manifestation of an implicit veto, enacted not through direct prohibition but through administrative control over maritime areas where China claims sovereignty. This situation compels telecommunication companies and Southeast Asian governments alike to reconsider political risk factors, even in seemingly neutral technical decisions. Thus, undersea cables, once primarily considered civilian infrastructure, are becoming deeply integrated into the soft coercion strategies of superpowers. Through bid vetoes, survey delays, route severances, or physical interference, the US and China are transforming the digital space into a silent front of coercive power, where each landing point or newly laid cable represents not just an investment decision but a strategic declaration of influence, control, and exclusion.

Strategic Ripples Beneath the Waves: How US-China Cable Rivalry Undermines Southeast Asia's Regional Security

The strategic rivalry between the United States and China over undersea cables in the South China Sea is not merely reshaping global digital connectivity but is also precipitating systemic non-traditional security challenges for Southeast Asia. As these cable routes become instruments for projecting influence, exercising strategic vetoes, and expanding soft control, this inherently civilian infrastructure is increasingly enmeshed in the security and defense calculus of major powers, placing intermediary nations in a complex geostrategic bind. Unlike conventional military conflicts, competition in the undersea cable domain unfolds within digital infrastructure, where power is often cloaked in technical, legal, or commercial guise. This "subterranean" characteristic, however, makes the attendant security risks more intractable and prone to being overlooked in strategic planning. In an era where undersea cables form the bedrock of digital commerce, finance, defense coordination, and information flows, any interference—from delaying survey permits and sabotaging cable routes to controlling data centers—can generate systemic risks for the entire regional security architecture.

For Southeast Asia, the crucial question is not one of alignment but rather of how to safeguard digital infrastructure, uphold digital sovereignty, and avoid entanglement in a vortex of strategic polarization. Amidst disparate levels of infrastructural development and deepening technological dependence among ASEAN member states, the US-China contest over undersea cables is generating profound and far-reaching impacts on the regional security architecture, both horizontally (across diplomacy, technology, and legal frameworks) and vertically (implicating sovereignty, trust, and collective security structures).

Expanding the "Subterranean Battlefield": From Territorial Disputes to Digital Infrastructure Contestation

Historically, the South China Sea has been a recognized arena for territorial and resource disputes, with major powers and littoral states vying for control over islands, shoals, fishing grounds, and strategic maritime lanes. The 21st century, however, has witnessed a power shift from the material to the digital, transforming the South China Sea into an emergent "subterranean battlefield". Consequently, control over undersea cables now transcends purely technological considerations, becoming a new emblem of spatial power and strategic presence. The US-China confrontation over undersea cables in the South China Sea has effectively broadened the competitive landscape from surface territorial claims to the seabed and its underlying infrastructure. Notably, China has utilized administrative and technical tools to assert its territorial claims by controlling seabed surveys, denying permits for international cable projects transiting disputed waters, and mandating the use of Chinese survey vessels for access to the region (Tan, 2023). These actions not only underscore China's capacity for a technical veto but also serve as a mechanism for Beijing to assert soft sovereignty without deploying drilling rigs or naval assets; merely obstructing cable installation allows for the indirect assertion of spatial control.

Conversely, the United States and its technology corporations have responded by redesigning digital connectivity maps, deliberately circumventing areas claimed by China or deemed vulnerable to its interference. This clearly manifests an effort to architect digital connectivity spaces aligned with geostrategic interests, thereby creating "infrastructure corridors" that compete with China's sphere of influence. When undersea cable infrastructure becomes inextricably linked to sovereignty claims, the maritime domain—once a conduit for digital exchange—metamorphoses into an arena of covert political strife. A cable route permitted through Chinese-claimed waters could be construed as de facto recognition of those claims; conversely, rerouting to avoid disputed areas might be perceived by Beijing as a hostile act. This dynamic politicizes and securitizes the digital space, triggering a cascade of repercussions for regional stability.

For Southeast Asian nations, this situation intensifies strategic pressures in selecting investors, contractors, and cable routes, as every technical decision is laden with geopolitical risk. An agreement to land a US-sponsored cable could provoke a Chinese backlash, while accepting a Chinese-funded project might elicit security concerns and tacit opposition from Washington. As a result, the regional strategic landscape is no longer clearly delineated along military-civilian lines but has become multi-layered, intricate, and fraught with "soft conflict" within the undersea infrastructure domain.

Heightened Risks of Infrastructure Disruption and Regional Digital Instability

Undersea fiber optic cable systems are indispensable for Southeast Asia's economic, political, and social connectivity with the global community. In an environment of accelerating digital transformation and e-commerce expansion, ASEAN countries are increasingly reliant on the resilience of transnational digital infrastructure. However, as the South China Sea becomes a strategic battleground for US-China competition over cable deployment, control, and veto power, the entire region confronts a novel threat: the structural disruption of digital infrastructure, with spillover effects extending far beyond the purely technical realm.

Firstly, the danger of connectivity interruptions—stemming from technical malfunctions, physical interference, or repair delays—is increasingly palpable. Key routes like the AAG (Asia-America Gateway), Intra-Asia (IA), and Asia Direct Cable (ADC), which traverse disputed maritime zones or pass near Chinese-controlled features, have frequently suffered incidents in recent years. More disconcerting is the growing capability of strategically motivated actors to physically interfere with cable systems. The majority of international cable routes converge at critical "chokepoints" within the South China Sea, where a single point of failure could affect five to seven nations in the region. In the event of conflict, even at a low intensity, the potential for undersea cables to be leveraged for coercion is undeniable.

In the long term, a lack of network consistency and resilience not only inflicts economic damage but also directly jeopardizes social stability, governmental operations, and national security. During prolonged cable outages, ASEAN member states—particularly those heavily dependent on foreign-based data centers and cloud services—would face information paralysis, disruptions to payment systems, turmoil in social media communications, and an erosion of public trust in state capacity. Should such disruptions coincide with periods of political instability, natural disasters, or economic crises, they could rapidly escalate into widespread domestic insecurity.

Challenges to Digital Sovereignty and National Cybersecurity

In the digital era, sovereignty extends beyond geographical borders and physical territory to encompass control over data, digital infrastructure, and national cyberspace. Against the backdrop of US-China rivalry for influence

via undersea cable systems, Southeast Asian nations confront a new genre of threat: the erosion of digital sovereignty and an escalation of structural cybersecurity risks.

(i) Many ASEAN countries, including Vietnam, the Philippines, Malaysia, and Indonesia, currently lack full ownership or control over international undersea cable routes transiting their maritime jurisdictions. A substantial portion of these cables are financed, designed, and operated by foreign corporations such as SubCom (USA), HMN Technologies (China), Google, or Meta. When recipient nations primarily function as co-financiers or landing point providers, their ability to influence operations, maintenance, encryption standards, and data security is inherently constrained (Capri, 2024). This implies that a nation's strategic data flows—including financial, defense, health, and public administration information—could be vulnerable to access, surveillance, or manipulation by external parties, while the host state may lack adequate tools for detection and response.

(ii) Technological dependence on foreign infrastructure providers creates intrinsic vulnerabilities in domestic cybersecurity posture. China frequently offers "turnkey" undersea cable solutions through companies like China Telecom, Hengtong, Huawei, or HMN Tech, often bundled with long-term technical support and maintenance. While this facilitates rapid access to high-speed connectivity for developing nations, it also cultivates a soft dependency on China's technological ecosystem (Noor, 2024). Over time, this reliance could lead to data exfiltration, cyber espionage, or information manipulation, particularly during political crises or external conflicts.

(iii) The contest between US and Chinese digital ecosystems is trapping Southeast Asian nations between two conflicting standards regimes, creating disarray in the formulation of domestic cybersecurity policies. On one hand, they face pressure to adhere to international standards promoted by the US and its allies (such as end-to-end encryption, data localization, and independent audits). On the other, they confront the allure of the Chinese model—characterized by lower costs, rapid deployment, and fewer legal encumbrances, albeit accompanied by risks of surveillance or censorship. This lack of normative consistency impedes many ASEAN countries from developing coherent, independent cybersecurity strategies aligned with their national interests.

Deepening Polarization and Eroding Strategic Trust within ASEAN

The Association of Southeast Asian Nations (ASEAN) has long pursued a strategic doctrine centered on maintaining its centrality within regional security architectures and upholding a balanced strategic posture vis-à-vis major powers. However, as US-China competition in undersea cable infrastructure intensifies in scope and depth, this inherently delicate neutral framework is increasingly strained by internal polarization, as member states are compelled to make technical choices laden with strategic implications.

Firstly, divergent selections of undersea cable partners have fostered two polarizing strategic currents within ASEAN. Some nations, such as Singapore, the Philippines, and Vietnam, are increasingly collaborating with US technology firms, prioritizing data security, interoperable standards, and aligning with initiatives like the PGII or Quad infrastructure projects. Conversely, countries like Cambodia, Myanmar, and Laos continue to embrace Chinese investment in telecommunications and data center projects, where financial terms are often more accommodative and regulatory oversight less stringent (Capri, 2024; Noor, 2024). This divergence in cable partnerships also reflects a broader strategic schism between nations favoring open, multilateral frameworks and those more vulnerable to being drawn into Beijing's proprietary technological sphere. Secondly, a deficit in transparency and coordination regarding decisions on landing points, data sharing protocols, and encryption standards further exacerbates trust deficits among ASEAN members. Thirdly, the cable competition also undermines ASEAN's ability to establish a common framework for digital sovereignty, maritime infrastructure security, and digital domain governance. Progress on initiatives such as the Code of Conduct in the South China Sea (COC), the ASEAN Cybersecurity Dialogue, or a regional data center has faltered due to conflicting national interests. Fourthly, in the long run, this polarization is not merely a passive consequence of US-China rivalry but constitutes a structural threat to ASEAN's strategic autonomy. When cable networks are deployed according to the logic of two antagonistic technological ecosystems, any ASEAN endeavor to construct a common or neutral connectivity system becomes increasingly unviable. The prevailing digital connectivity architecture, rather than fostering regional cohesion, is actively reproducing strategic cleavages within ASEAN, thereby presenting an urgent imperative for the bloc to redefine its central role in a rapidly transforming regional security order.

Cooperation or Alignment: The Strategic Dilemma of Southeast Asian Nations

As US-China strategic competition extends from trade and military domains into the realm of digital infrastructure, particularly undersea fiber optic systems, Southeast Asian nations are no longer peripheral spectators but increasingly pivotal actors in strategic decisions that will shape the region's future.

As intermediary states situated along critical trans-Pacific cable routes and maintaining intricate economic and security ties with both superpowers, ASEAN countries face a classic strategic dilemma: (1) deeper cooperation

with the United States risks economic and political blowback from China; and (2) gravitation towards Chinese-built infrastructure risks exclusion from US-influenced global digital networks and a compromise of digital sovereignty. A distinctive aspect of this predicament is that ostensibly technical decisions—such as selecting cable routes, deployment partners, or maintenance providers—carry profound geopolitical undertones, rendering any action liable to be interpreted as "choosing sides". However, given limited indigenous technical capabilities, internal political rifts, and varying degrees of external dependence among ASEAN members, sustaining a unified stance becomes exceedingly difficult. This "cannot remain disengaged, yet cannot definitively choose" scenario engenders a unique strategic impasse, reflecting the inherent constraints of a "soft neutrality" policy amid systemic technological rivalry.

In international strategic theory, medium-sized states with limited capabilities and high dependence on the external environment frequently encounter such strategic dilemmas within competitive international systems. This is particularly acute in the current US-China rivalry, where the confrontation has permeated the digital infrastructure layer, with undersea cables becoming a decisive arena for shaping global network power (Farrell & Newman, 2019; Capri, 2024). Southeast Asian nations, at the geographical nexus of trans-Pacific cable routes, have become an indispensable strategic space in the calculations of both Washington and Beijing. The paradox is that ASEAN countries can neither remain disengaged nor can they unequivocally choose sides. On one hand, they have a vital interest in maintaining a stable, secure, and diversified digital connectivity environment. On the other hand, any decision—from selecting cable installation partners and approving survey missions to determining equipment maintenance protocols and encryption standards—is liable to be interpreted by the major powers as a political signal.

Unlike the Cold War, where nations could maintain "hard neutrality" through military non-alignment, contemporary technical decisions, however ostensibly neutral, carry unavoidable strategic implications. This creates a novel form of "technological dilemma", where power hinges not on military might but on data, source codes, technical standards, and cable landing station locations. The contention lies not in a nation's political will but in the very infrastructure upon which it depends—a structural constraint that even traditionally neutral states like Singapore cannot entirely escape. This situation is further complicated by significant disparities in technical autonomy and domestic technological capabilities among ASEAN member states. Some countries, like Vietnam, Indonesia, and Malaysia, may pursue a "multi-vector non-aligned" policy for certain undersea cable projects. However, smaller nations like Laos, Cambodia, or Myanmar often have little alternative but to accept investments from readily available sources, typically China or its affiliated companies. Meanwhile, the Philippines increasingly aligns with the US on both infrastructure and security, fracturing the regional landscape not only along geopolitical lines but also according to digital control capabilities. Consequently, the "soft balancing" strategy pursued by many ASEAN nations is becoming progressively harder to sustain. While countries may attempt to cooperate with both the US and China in different sectors, in the realm of undersea cables, the "coexistence of two systems" is almost operationally untenable. At some point, nations will be compelled to choose: either security aligned with US standards or lower costs coupled with Chinese technical oversight.

In essence, within the weaponized domain of undersea cables, strategic ambiguity is no longer a viable long-term option. Southeast Asian nations will inevitably confront a series of increasingly sensitive decisions, where each technical choice is a de facto strategic one. This encapsulates the profound nature of the strategic dilemma facing intermediate states: "not controlling the game, yet any move can alter the digital power map".

Confronted by mounting pressure from US-China rivalry in digital infrastructure, ASEAN member states have adopted varied strategic responses, contingent on their geopolitical positions, economic conditions, technical capabilities, and foreign policy orientations. These divergences are evident not only in official pronouncements but also in their approaches to undersea cables—particularly in selecting deployment partners, landing sites, ownership models, and operational frameworks. This has yielded a spectrum of strategic postures, from "overt alignment" to "soft balancing" and "flexible neutrality", underscoring ASEAN's internal strategic fragmentation under systemic duress. Specifically:

(i) Singapore leans towards the United States from a position of advanced technological neutrality. As Southeast Asia's premier data transit hub, Singapore hosts and operates over 25 international undersea cables and major data centers for global tech giants like Google, Meta, Microsoft, and Amazon (Capri, 2024). In US-allied sponsored projects such as Apricot, Echo, and Bifrost, Singapore is a pivotal landing point, cementing its role as the region's digital nexus. While permitting some technological cooperation with China (e.g., Huawei's data center), Singapore demonstrably prioritizes a transparent, high-security connectivity ecosystem aligned with Western standards. Rather than explicit political declarations, it employs a model of "sophisticated neutrality", avoiding overt alignment in its foreign policy.

(ii) The Philippines has opted for comprehensive cooperation with the United States on both infrastructure and strategy. Under President Ferdinand Marcos Jr., the Philippines has unequivocally signaled its pro-US orientation through enhanced defense cooperation (including EDCA expansion and increased US military

presence) and its digital infrastructure choices. The SEA-US, Bifrost, and Apricot cables all land in the Philippines, financed by American, Japanese, and Singaporean investors. The Philippine government has also resolutely excluded Chinese suppliers from strategic national projects (Tan, 2023). This indicates a Philippine inclination not only towards military alignment with the US but also towards active integration into the US-Japan digital network as part of a broader alliance restructuring.

(iii) Cambodia and Myanmar have accepted strategic dependence on China. With limited domestic infrastructure and close political ties to Beijing, both Cambodia and Myanmar have become key recipients of Chinese investment in cables, data facilities, and telecommunication systems. For example, Cambodia relies almost entirely on Huawei-supplied 5G infrastructure; Myanmar, particularly since its 2021 coup, has intensified technological cooperation with China for cyberspace surveillance and communications control (Cannon, 2024). This model offers lower initial investment and rapid deployment but fosters strategic dependence on China's technological ecosystem, affording these nations minimal latitude for independent digital policy.

(iv) Vietnam, Indonesia, and Malaysia pursue a calculated soft balancing strategy. These nations strive to maintain a delicate equilibrium with both major powers. Vietnam has embraced cable projects backed by Google and Meta (e.g., IA, and SEA-ME-WE-6 post-Chinese exclusion) while allowing some technical infrastructure cooperation with China via subsidiaries or non-political investments. Indonesia, a key node for the Bifrost cable, demonstrates a selective approach to international partners, aiming to avert over-dependence. Malaysia exhibits similar tendencies, coordinating with multiple stakeholders to diversify risk. These countries seek strategic equidistance from both the US and China, eschewing overt alignment while prioritizing high technical security standards when necessary.

This diversity in national responses not only reflects individual strategic calculations but also exposes a lack of cohesion in ASEAN's collective approach to digital infrastructure competition. This, in turn, creates significant challenges in formulating common policies on digital sovereignty, regional security, and undersea cable technical coordination. The tendency for individual nations to "negotiate" separately with superpowers renders ASEAN susceptible to internal polarization and weakens its collective bargaining position vis-à-vis the United States or China. This reality inherently constrains cooperation among Southeast Asian nations in the undersea cable domain.

In a global order increasingly polarized by competing technological networks and infrastructure rivalries, Southeast Asian nations have long advocated "technological neutrality" to avoid entanglement in the US-China geopolitical contest. However, practical realities demonstrate that sustaining neutrality in undersea cable infrastructure is becoming increasingly untenable, primarily due to the inherently politicized nature of modern technology. Unlike traditional sectors like diplomacy, trade, or defense, where alignments can be more readily discerned, selecting a cable partner is often ostensibly a purely technical decision. Yet, in practice, choices regarding deployment companies (e.g., SubCom vs. HMN Tech), landing sites (e.g., Guam vs. Hainan), encryption standards (e.g., AES 256-bit vs. domestic protocols), and even repair mechanisms are all imbued with profound strategic significance. This compels even neutrality-aspiring nations to make choices with geopolitical implications, whether indirect or unintentional. Pressure intensifies as neither the US nor China tolerates "prolonged ambiguity" in regional states' policies and actions. Washington has urged partners to exclude Chinese firms from critical projects like SEA-ME-WE 6 or sever connections with Hong Kong data centers (Brock, 2023; Capri, 2024). Conversely, China employs administrative levers—delaying surveys, complicating permits, offering conditional infrastructure packages—to create a complex web of counter-pressures, compelling nations to act, even without formal declarations of allegiance.

Another inherent limitation of "technological neutrality" is the insufficient indigenous capacity of most Southeast Asian nations. Deficiencies in core technological autonomy, finance, infrastructure, and skilled personnel prevent many from effectively implementing a truly neutral strategy. Furthermore, the global technological ecosystem is increasingly fragmented. US-Japan-Australia affiliated cable networks utilize operating systems, encryption, and governance distinct from China-Russia-Pakistan-Iran systems. These disparities in standards, access, routing, and data storage render networks technically incompatible, precluding neutral coexistence within a single jurisdiction without operational conflicts or political risks. Ultimately, even if a country maintains policy neutrality, it cannot control the political interpretation of its technical actions. A maintenance contract with SubCom might be seen by Beijing as pro-Western alignment; collaboration on surveys with HMN Technologies could prompt Washington to restrict infrastructure investment. This underscores the stark reality: in the contested domain of undersea cables, no "apolitical" technological space exists, as infrastructure itself has become an integral component of soft power, structural influence, and coercion.

Given the escalating pressures from US-China digital infrastructure rivalry, it is evident that individual ASEAN member state responses—whether alignment or attempted neutrality—do not foster a stable, autonomous regional security architecture. While personalized strategies may optimize short-term national interests, they risk exacerbating internal bloc polarization, creating asymmetric technological dependencies, and undermining ASEAN's collective bargaining power with major powers. In this context, ASEAN faces an urgent imperative to

transcend its reactive posture and forge a form of "collective digital sovereignty"—akin to a mutual defense mechanism for an era of fragmented infrastructure and politicized technology. We propose that several existing mechanisms could be expanded and transformed into such a regional digital sovereignty framework:

Firstly, ASEAN and its member states could collaboratively develop a common set of technical standards for undersea cable security and operation, stipulating clear requirements for encryption, data governance, access rights, and storage. These standards must hold regional validity and be binding on all external partners deploying infrastructure within ASEAN territory. This would empower ASEAN to reassert control over digital rules of engagement and avoid entanglement in conflicting technological ecosystems.

Secondly, the establishment of an "ASEAN Subsea Cable Resilience Fund", financed by member states and development partners, is crucial. This fund would support maintenance, monitoring, and rapid response to cable incidents, reducing dependence on foreign-owned repair vessels (which are susceptible to strategic manipulation, like Chinese vessels). This mechanism would parallel disaster relief funds but focus specifically on digital infrastructure.

Thirdly, ASEAN should expedite the creation of an independent regional data center, managed by a dedicated regional technical body and located in a neutral member state like Brunei or Malaysia. This center would serve as a repository for essential, minimal regional-level data, mitigating risks associated with concentrating all data in major power-operated centers.

Fourthly, ASEAN can leverage and enhance existing frameworks like the ASEAN Digital Masterplan 2025, the ASEAN Cybersecurity Cooperation Strategy, or the ADMM+ to encompass cable infrastructure, build national digital defense capacities, and facilitate intelligence sharing on cable sabotage risks—an area where ASEAN currently lacks robust formal mechanisms.

Crucially, establishing collective digital sovereignty would enable ASEAN to transition from being a rule-taker to a rule-maker, from passively choosing sides to proactively shaping the regional digital environment according to its collective interests. This represents not merely an escape from the current strategic dilemma but a strategic leap towards reaffirming ASEAN's centrality in the 21st-century regional security architecture—achieved not through military might, but through the capacity for independent, multilateral, and sovereign governance of its digital infrastructure.

CONCLUSION

The US-China rivalry over undersea cables in the South China Sea transcends technological competition—it is a defining manifestation of global power restructuring in the digital domain. As these cables are weaponized to control data flows, assert influence, and exercise strategic vetoes, civilian infrastructure has become a battleground for covert geopolitical maneuvering.

For Southeast Asian nations, neutrality is no longer a tenable position when every technical decision—from cable routing to data center partnerships—carries embedded strategic consequences. The region now faces a stark imperative: to move beyond passive alignment and toward active stewardship of its digital destiny.

ASEAN's path forward lies not in choosing sides, but in collectively shaping the digital domain through a framework of shared sovereignty, technical standards, and regional resilience. Only by institutionalizing collective digital sovereignty can ASEAN reclaim its agency, mitigate polarization, and secure its centrality in the evolving Indo-Pacific security architecture—not through military might, but through sovereign, multilateral governance of its digital future.

Acknowledgments

This research is funded by University of Foreign Language Studies, The University of Da Nang under project number T2024-05- 14

REFERENCES

Baraniuk, C. (2025). Subsea fibre cables can 'listen out' for sabotage. BBC. https://www.bbc.com/news/articles/cn52rglxr62o

Brock, J. (2023). U.S. and China wage war beneath the waves – over internet cables. Reuters. https://www.reuters.com/investigates/special-report/us-china-tech-cables/

Cannon, B. (2024). Undersea cable security in the Indo-Pacific: Enhancing the Quad's collaborative approach. Marine Policy, 171. https://doi.org/10.1016/j.marpol.2024.106415

Capri, A. (2024). The New Geopolitics of Undersea Cables. Hinrich Foundation. https://www.hinrichfoundation.com/research/wp/tech/the-new-geopolitics-of-undersea-cables/

CSIS. (2023). China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts. https://www.csis.org/analysis/chinas-underwater-power-play-prcs-new-subsea-cable-cutting-ship-spooks-international

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351

Geri, M. (2023). South China Sea tensions conceal a secret war to control the world's Internet. Euractiv. https://www.euractiv.com/section/global-europe/opinion/south-china-sea-tensions-conceal-a-secret-war-to-control-the-worlds-internet/

McCartney, M. (2024). Is China Hacking Undersea Cables? What We Know. Newsweek. https://www.newsweek.com/china-hacking-undersea-cables-1902970

Noor, M. (2024). Undersea cables and the vulnerability of American power. Newsweek. https://www.newsweek.com/china-hacking-undersea-cables-1902970

Runde, D. (2023). Subsea Cables: Strategic Infrastructure in the Digital Age. CSIS. https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Scobell, A. (2018). The South China Sea and US–China Rivalry. Political Science Quarterly, 133(2), 209.

Tan, R. (2024). Escalating contest over South China Sea disrupts international cable system. The Washington Post. https://www.washingtonpost.com/world/2024/10/03/south-china-sea-underwater-cables/

Telegeography. (2024). Submarine Cable Map. https://www.submarinecablemap.com/

The Washington Post. (2023, October 3). Escalating contest over South China Sea disrupts international cable system. https://www.washingtonpost.com/world/2023/10/03/south-china-sea-underwater-cables

Zhang, J. (2024). Heading in the direction of bifurcated networks: Hong Kong's evolution amidst the global submarine cable system. Asian Review of Political Economy, 3(8). https://doi.org/10.1007/s44216-024-00029-1

Zhang, J., & Hou, C. (2024). Status, Challenge and Responses of Global Deep-Sea Infrastructure Governance. Pacific Journal, 32(4), 74–88.

Zheng, H. (2024). The U．S． Undersea Cable Rivalry with China: Strategic Operation and Impact Evaluation. Pacific Journal, 32(6), 93 – 106.

