Atlantic Council
SCOWCROFT MIDDLE EAST SECURITY INITIATIVE

ISSUE BRIEF

CHINA'S SUBSEA-CABLE POWER PLAY IN THE MIDDLE EAST AND NORTH AFRICA

MAY 2023 DALE ALUF

Executive summary

The Middle East and North Africa (MENA) has become increasingly connected to submarine cable networks owned, built, or upgraded by Chinese firms. Since they entered the market in the late '90s, Chinese companies have constructed, upgraded, or acquired ownership stakes in thirteen of some sixty-two cables traversing MENA, forging fifty-seven connections at thirty-nine landing stations. In 2025, another (SeaMeWe-6) will go online, raising the total to sixty-one connections at thirty-nine MENA landing stations.[1] Submarine cables are among the most critical digital infrastructures, serving as conduits for more than 95 percent of international data flows and communications, including an estimated $10 trillion in financial transfers daily.[2] With China aiming to capture 60 percent of the cable market by 2025, MENA could become increasingly reliant on Chinese networks to transmit sensitive data.[3]

These cables are strategically important to MENA countries, particularly those striving to digitize their economies. With bandwidth demand steadily rising across the region, governments have been increasingly looking to China for digital infrastructure. MENA countries have also welcomed these connections as a means to diversify their networks—reducing dependence on US/Western cables. As home to one of three critical cable choke points—the Suez Canal-Red Sea-Mandab Strait passage—the Middle East and North Africa region is of geostrategic significance to China. These cables form part of the Digital Silk Road and connect China's transregional assets (military and civilian), along

The Atlantic Council's work on Middle East security honors the legacy of Brent Scowcroft and his tireless efforts to build a new security architecture for the region. Our work in this area addresses the full range of security threats and challenges including the danger of interstate warfare, the role of terrorist groups and other nonstate actors, and the underlying security threats facing countries in the region.

1 The term cable landing station is used to describe physical locations where one or more submarine telecommunication cables make landfall and connect to land-based power and networking infrastructure.

2 Morcos, P., and C. Wall. "Invisible and Vital: Undersea Cables and Transatlantic Security." Center for Strategic & International Studies 11 (2021). https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

3 J. E. Hillman. "War and PEACE on China's Digital Silk Road," Center for Strategic And International Studies, May 16, 2019, https://www.csis.org/analysis/war-and-peace-chinas-digital-silk-road

the Belt and Road Initiative (BRI).[4] Ensuring high-speed, low-latency connectivity is vital in optimizing and maintaining the integrity of supply chains and other activity that supports economic growth. Chinese energy imports from MENA, and much of its trade from the region and Europe, travel through the Suez Canal-Red Sea-Mandab Strait passage. The Pakistan and East Africa Connecting Europe (PEACE) fiber-optic cable, a network funded, owned, and constructed entirely by Chinese entities, was built specifically to complement the BRI. It connects Chinese assets (the $62 billion infrastructure project known as the China Pakistan Economic Corridor) in Gwadar, Pakistan, to Djibouti, which hosts a Chinese naval base, and runs through the Middle East and onward to Europe. PEACE would harbor immense strategic significance for China even if it were not commercially viable because it supports and enhances the People's Liberation Army's ability to project power.

Like other nations, China's undersea cables are essential in coordinating military operations. Most military communications travel along these networks, making them susceptible to eavesdropping. The strategic political-economic importance of the MENA region has made it an attractive place for cable espionage. The networks that pass through the Suez are among the busiest in terms of telecommunications traffic and, therefore, surveillance. As China's robust economic presence and modest military presence both expand, reliable signals intelligence will become ever more important to Beijing. At the same time, the development of increasingly advanced military equipment continues to drive demand for more reliable and secure bandwidth. China has sought to leverage underwater cable systems to detect submarines by fitting them with monitors and sensors.[5] While this endeavor began with a so-called underwater great firewall near China's borders, Beijing has indicated that its aspirations for the system are global.

These underwater observation systems could complicate US and MENA countries' regional naval operations. These developments concern Israel and Gulf countries as China could share information gleaned from these systems with its strategic partner, Iran: their twenty-five year cooperation agreement includes commitments to intelligence sharing and allows China to utilize an Iranian port, Jask, on the Gulf of Oman. With tensions between China and the West showing no signs of abating, Chinese cables traversing MENA could emerge as a contentious issue in the geopolitics of the internet. Already in recent years, the United States and Australia have intervened to prevent the rollout of cables by Chinese companies in the Pacific. PEACE has not escaped the attention of American policymakers: it featured prominently in a Senate Foreign Relations Subcommittee hearing on the Middle East as recently as August 4, 2022. Senator Bill Hagerty raised concerns surrounding the Chinese Communist Party's ability to cut it, disrupt it, divert it, and monitor the information of allies and suggested that the US State Department examine the measures taken by the previous administration to secure SeaMeWe-6. These measures included a $3.8M training grant offered by the US Trade and Development Agency (USTDA) to five telecom firms on the cable's route, contingent on them choosing American SubCom over HMN-Tech, along with warnings from US diplomats about HMN-Tech's security risks and impending sanctions on the Chinese company that would put the telecom carriers' cable project investment at risk. The measures worked, and Subcom was selected over HMN Tech to build SMW6.

China wants to reduce its dependence on foreign cables while making other countries more dependent on Chinese networks. China's growing presence in MENA's cable industry is significant because Beijing has the power to shape the route of global internet traffic by determining when, where, and how to build cables. For a country that seeks to alter the internet's physical form and influence digital behavior while exerting supreme control over information flows, the dominance of the undersea cable network provides significant strategic advantages. Until now, the issue of who controls 5G in MENA has overshadowed other information and other technologies, with ports sometimes added to the mix. However, considering the US strategic reorientation to increase its engagement with the Middle East to

4 The Digital Silk Road (DSR), first introduced in a whitepaper jointly issued by China's National Development and Reform Commission (NDRC), Ministry of Foreign Affairs, and Ministry of Commerce in 2015, is a component of the Belt and Road Initiative. Digital projects that began prior to the DSR's conception have since been folded under the initiative.

5 C. Wong, "'Underwater Great Wall': Chinese firm proposes building network of submarine detectors to boost nation's defense," South China Morning Post, May 19, 2016, https://www.scmp.com/news/china/diplomacy-defence/article/1947212/underwater-great-wall-chinese-firm-proposes-building.

counter China, particularly in advanced technology, MENA's subsea cables are poised to attract more attention. PEACE, in particular, is poised to emerge as a flashpoint in the Sino-American internet feud.

Introduction: Chinese industry growth meets MENA digitization

As an aspiring "cyber superpower," China recognizes the vital importance of submarine cables and has expended considerable resources to expand its presence in the sector. As host to one of three critical cable choke points—the Suez Canal-Red Sea-Mandab Strait passage—the Middle East and North Africa (MENA) region is important for China's digital connectivity strategy. In China's first foray into the industry, China Telecom partnered with France Telecom to install the world's longest submarine fiber system, Sea-Me-We 3 (South East Asia-Middle East-Western Europe). The 39,000 kilometer (km) network first went online on September 30, 1999. Of Sea-Me-We 3's thirty-nine cable landing points, two are in Egypt (Alexandria and Suez), with others landing in Morocco, Turkey, Saudi Arabia, Djibouti, Oman, and the United Arab Emirates. Since then, Chinese companies have constructed, upgraded, or acquired ownership stakes in thirteen of some sixty-three cables traversing MENA (see table 1), forging fifty-seven connections at thirty-nine landing stations.[6] Provided China Unicom and PCCW remain in the SeaMeWe-6 cable consortium, it will add another to the list of Chinese companies with stakes in MENA networks. Slated for completion in 2025, SeaMeWe-6 will add four links in the region, bringing the total number of connections to sixty-one at thirty-nine MENA landing stations.

China's expanding presence in MENA's subsea cable network is commensurate with its growth in the sector globally. Sea-Me-We 3 was a manifestation of a policy that China's central government was formulating during the '90s under the leadership of President Jiang Zemin: Going Global. The plan not only gave the green light for Chinese companies to expand their operations worldwide but also included robust policy support and preferential funding to realize this aspiration.[7] Now, under President Xi Jinping, Chinese telecom companies continue to enjoy strong government support through initiatives like the Digital Silk Road—the virtual component of BRI.

Rewind two decades and China was almost absent from the undersea cable industry and depended mostly on foreign companies. Today, Chinese firms have emerged as leading providers of this vital infrastructure.[8][9] China's HMN Tech (formerly Huawei Marine) managed to secure more than one hundred contracts in the subsea cable sector since its founding in 2008. A 2020 report by the US Federal Communications Commission (FCC) points out that HMN Tech has "built or repaired almost a quarter of the world's cables."[10] Today, five Chinese state—controlled entities—China Telecom, China Unicom, China Mobile, CTM, and National Grid Corporation of the Philippines—along with Hong Kong based PCCW enjoy ownership stakes in thirty-three of the 545 cables globally (at the time of writing).[11] [12] [13] According to Leiden Asia Center research, China is a landing point, owner, or supplier for 11.4 percent

6 "Submarine cable map," TeleGeography, licensed under CC BY-SA 4.0, 2022. Accessed March 07, 2023. https://www.submarinecablemap.com/.

7 M. van der Stelt and E. Blaauw et al., "The driving forces behind China's foreign policy—has China become more assertive?," RaboResearch-Economic Research, Rabobank, n.d., https://economics.rabobank.com/publications/2013/october/the-driving-forces-behind-chinas-foreign-policy-has-china-become-more-assertive/.

8 J. Hemmings, "Reconstructing order: The geopolitical risks in China's Digital Silk Road," Asia Policy 27, no. 1 (2020): 5-21.

9 L. Burdette, "Leveraging submarine cables for political gain: US responses to Chinese strategy," *Journal of Public & International Affairs*, May 5, 2021, https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy.

10 Federal Communications Commission, "Process reform for executive branch review of certain FCC applications and petitions involving foreign ownership," 2020, https://docs.fcc.gov/public/attachments/FCC-20-133A1.pdf.

11 These companies are China Mobile, China Telecom, China Unicom, Citic Telecom International, CTM, and National Grid Corporation of the Philippines. Source: Aggregated data from SIGNAL's dataset.

12 China Unicom holds an 18% interest in PCCW. It's not clear to what degree China Unicom is able to influence PCCW operations and decision making. However, several high-level executives sit on the PCCW's board of directors.

13 In November 2019, an internal Filipino government report alleged that the National Grid Corporation of the Philippines, partly owned by a Chinese state-owned electrical company, was in fact "under the full control" of the Chinese government, according to CNN. Source: James Griffiths, "China can shut off the Philippines' power grid at any time, leaked report warns," CNN, November 26, 2019, https://edition.cnn.com/2019/11/25/asia/philippines-china-power-grid-intl-hnk/index.html

Table 1: Submarine cables owned, financed, constructed or upgraded by Chinese companies in MENA

Cable	Online	Chinese Entity / Entities	Involvement	MENA Landing Stations
Sea-Me-We 3	1999	China Telecom; PCCW (HK); CTM	Part owners, consortium.	Djibouti City, Djibouti; Alexandria and Suez, Egypt; Tétouan, Morocco; Muscat, Oman; Jeddah, Saudi Arabia; Marmaris, Turkey; Fujairah, United Arab Emirates (UAE).
MedNautilus submarine system	2001	HMN Tech	Upgrade	Haifa and Tel Aviv, Israel; Istanbul, Turkey.
Transworld (TW1)	2006	HMN Tech	Upgrade	al-Seeb, Oman; Fujairah, UAE.
HANNIBAL System	2009	HMN Tech	Construction	Kelibia, Tunisia
Tobruk-Emasaed cable system	2010	HMN Tech	Construction	el-Quawef and Tobruk, Libya.
TE North/TGN-Eurasia/SEACOM/-Alexandros/Medex	2011	PCCW (HK)	Operations (Medex branch)	Abu Talat, Egypt; Annaba, Algeria.
Silphium	2013	HMN Tech	Construction	Derna, Libya.
Sea-Me-We 5	2016	China Mobile; China Telecom; China Unicom;	Part owners, consortium.	Haramous, Djibouti; Abu Talat and Zafarana, Egypt; Qalhat, Oman; Yanbu, Saudi Arabia; Marmaris, Turkey; Fujairah, UAE; al-Hudaydah, Yemen.
Asia-Africa-Europe 1 (AAE-1)	2017	China Unicom	Part owner, consortium funding.	Aden, Yemen; Djibouti City, Djibouti; Abu Talat, and Zafarana, Egypt; Doha, Qatar; Jeddah, Saudi Arabia; Fujairah, UAE; al-Bustan, Oman.
Gulf2Africa (G2A)	2017	HMN Tech	Upgrade	Salalah, Oman; Berbera and Bosaso, Somalia.
PEACE Cable	2022	Hengtong Group; China-ASEAN Information Harbor; China Construction Bank; HMN Tech PCCW Global	Owner Funding Construction Equipment Operation	Djibouti City, Djibouti; Abu Talat and Zafarana, Egypt; Jeddah, Saudi Arabia. [Also lands at Gwadar, Pakistan.]
2Africa	2023	China Mobile	Part owner, consortium.	Manama, Bahrain; Djibouti City, Djibouti; Port Said, Ras Ghareb, Suez, and Zafarana, Egypt; al-Faw, Iraq; Barka, Oman; Salalah, Oman; Doha, Qatar; al-Khobar, Duba, Jeddah, and Yanbu, Saudi Arabia; Port Sudan, Sudan; Abu Dhabi and Kalba, UAE.
SeaMeWe-6	Expected 2025	China Unicom PCCW	Part owner, consortium.	Djibouti City, Djibouti; Port Said and Ras Ghareb, Egypt; Yanbu, Saudi Arabia.

Source: Aggregated data from SIGNAL's dataset.

of global submarine cable networks; when including planned cables that figure increases to 24 percent.[14]

These critical components of internet architecture are of immense strategic significance for the MENA nations in which they land. Undersea cables link these countries and the continents of the world together, forming the "backbone" for international data connectivity. Today's global cable networks span roughly 1.3 million km. These "information superhighways" provide the high-bandwidth connections needed for a wide range of activities vital for modern society to function properly. As nations across MENA digitize their economies, demand for capacity (speed and bandwidth) has steadily increased. Moreover, COVID-19 catalyzed a shift in internet traffic patterns, generating greater volumes of data flows that have further increased demand.[15] MENA's economies can benefit from a 46 percent rise in gross domestic product (GDP) per capita over thirty years if fully digitalized, according to a 2021 World Bank report; this amounts to a $1.6 trillion benefit over the long term.[16] The increase in GDP would be more pronounced in the region's lower-income countries (by at least 71 percent), as gains are driven by closing the access gap to digital technologies. However, these projections are contingent upon ensuring access to high-quality, reliable cable connectivity.

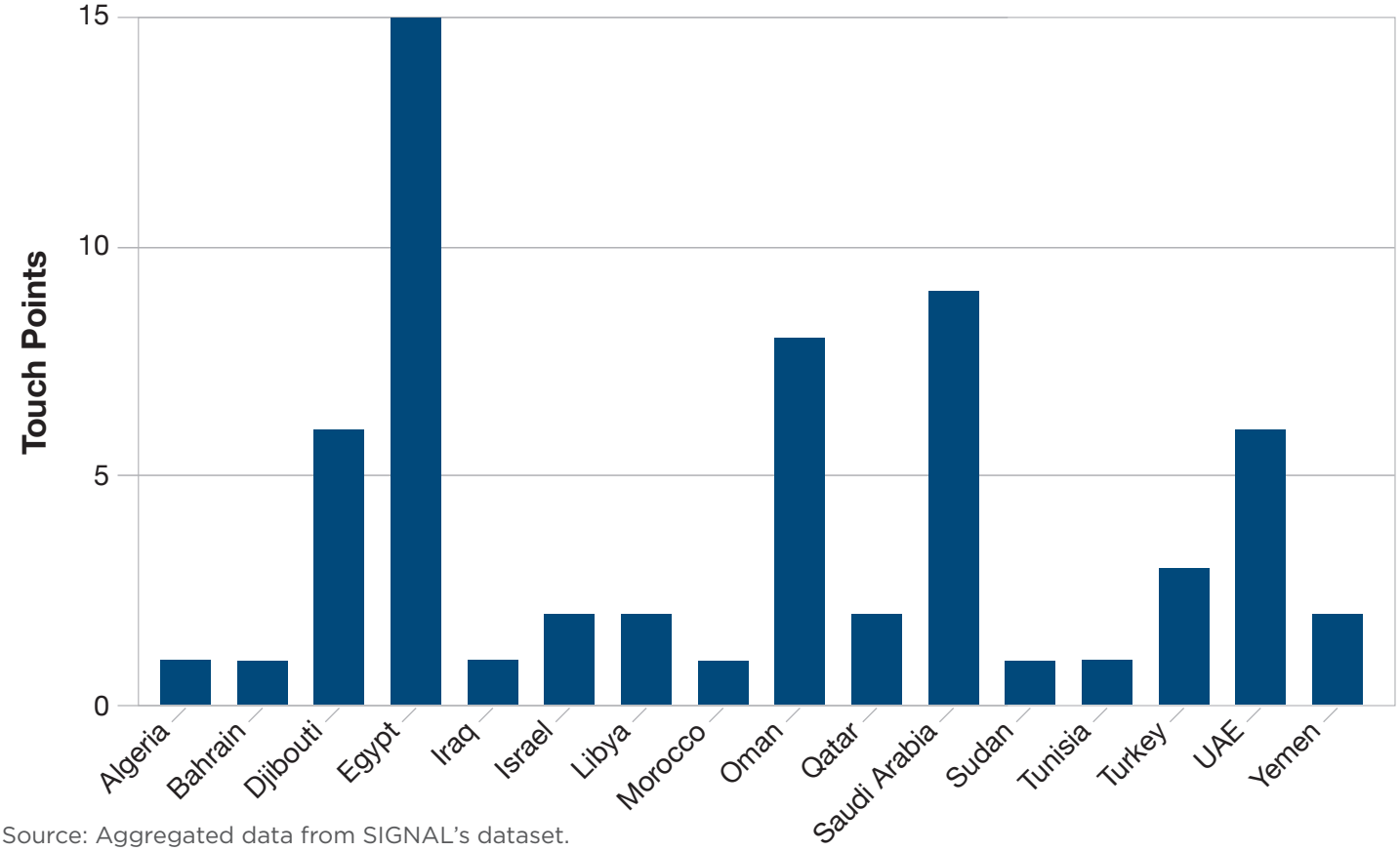
The MENA region has experienced the consequences of disruption to the subsea-cable network firsthand. In March 2013, two separate instances of politically motivated sabotage were executed on cables landing

14 Ghiasy, Richard, and Rajeshwari Krishnamurthy. "China's Digital Silk Road: Strategic Implications for the EU and India." Special Report 208 (2020). https://leidenasiacentre.nl/wp-content/uploads/2021/01/LAC-IPCS-DSR-Report-Aug-2020.pdf .

15 M. P. Goodman and M. Wayland, "Securing Asia's subsea network: U.S. interests and strategic options," Center for Strategic and International Studies, April 5, 2022, https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options.

16 A. P. Cusolito et al., *The upside of digital for the Middle East and North Africa: How digital technology adoption can accelerate growth and create jobs*, World Bank, 2021, https://openknowledge.worldbank.org/bitstream/handle/10986/37058/9781464816635.pdf?sequence=10&isAllowed=y.

Figure 1: Touch points at MENA landing stations of cables owned, built, or upgraded by Chinese entities (current and expected, 2023-25)



Source: Aggregated data from SIGNAL's dataset.

in Egypt. Egypt suffered a 60 percent reduction in internet communications as a result of the first incident, involving the Seacom cable, which connects Africa and Europe.[17] More recently, a single line that a ship's anchor severed off the coast of Yemen in 2020 wiped out 80 percent of the country's internet capacity.[18] As Helene Fouquet points out in the US magazine *Wired*, "though the country still had that last 20 percent, trying to route a water main of web traffic through a drinking straw resulted in near-total connectivity failure."[19] And the effects of the more recent incident resonated across the region, with Kuwait, Saudi Arabia, Sudan, and Ethiopia experiencing slowdowns in internet speeds. More cable connections in the region would add a layer of protection against such disruption: if a cable is damaged or a country with control over a line decides to choke the network, operators could redirect traffic.

By allowing Chinese cables to land on their shores, MENA states are diversifying their cable networks, reducing reliance on Western suppliers that have traditionally dominated the market. The subject of such diversification garnered substantial attention in 2013. As Lane Burdette explains in a 2021 paper published by the *Journal of Public and International Affairs*: "After the 2013 Snowden Disclosures revealed widespread US and partnered espionage using submarine cables, many states sought to decrease their

17 D. Shama, "Internet cable-cutters caught by Egypt signal new terror threat," *Times of Israel*, March 29, 2013, https://www.timesofisrael.com/internet-cable-cutters-caught-by-egypt-signal-new-terror-threat/.

18 H. Fouquet, "Cut undersea cable plunges Yemen into days-long internet outage," *Wired*, 2020, https://www.wired.com/story/yemen-internet-blackout-undersea-cable/.

19 Fouquet, "Cut undersea cable."

dependency on US infrastructure or cables landing on US shores."[20] According to Burdette, "China's Belt and Road Initiative (BRI) offered an attractive alternative for internet infrastructure financing, particularly to the developing world."[21] According to Mercator Institute for China Studies research, Chinese entities provided $7 billion in loans and foreign direct investment between 2013 and 2019 for global fiber-optic cable and telecommunication network projects.[22]

Edward Snowden's leaks of top-secret US National Security Agency (NSA) information illuminated the exploitation of submarine cables for intelligence and political purposes firsthand.[23] Perhaps ironically, the United States and other Western powers have raised concerns that China's growing presence in the undersea cable industry could threaten their national security and that of their allies. With industrial policies like Made in China 2025 setting the goal for Chinese companies to capture nearly a third of the cable market, MENA will likely find itself increasingly entangled in Chinese submarine cable networks. As such, it is important that countries in the region cultivate a deeper understanding of Chinese strategic thinking regarding submarine cables and the potential geopolitical consequences of Beijing's growing involvement in their internet architecture. Examining the Pakistan and East Africa Connecting Europe fiber-optic cable (PEACE), which traverses MENA, is instructive.

PEACE buttressing BRI

In a 2015 white paper, China's National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce announced: "[China] should jointly advance the construction of cross-border optical cables and other communications trunk line networks, improve international communications connectivity, and create an Information Silk Road." The document calls on Chinese entities to "build bilateral cross-border optical cable networks at a quicker pace, plan transcontinental submarine optical cable projects, and improve spatial (satellite) information passageways to expand information exchanges and cooperation."[24] Given that statements by China's leadership generate movement, it was little surprise that several months later, Chinese companies announced their plans to construct PEACE: a sprawling 25,000 km fiber-optic network designed to complement Xi's signature Belt and Road Initiative. Once complete,[25] PEACE will provide the shortest length and latency route connecting Asia, Africa, and Europe.[26]

The cable's creation has been a strictly Chinese-led venture. In June 2016, China Unicom led the creation of China-ASEAN Information Harbor Co. Ltd, a State Council-approved, state-owned enterprise (SOE), with China Unicom as the majority shareholder (45 percent). A year later, the newly formed company partnered with Tropic Science Co. Ltd and secured financing from China Construction Bank to fund PEACE. Meanwhile, China's HMN Tech has provided equipment for 15,000 km of the cable network. PEACE is privately owned by Hengtong Group—a company that has not been shy about its close ties to the Chinese Communist Party and cooperation with the People's Liberation Army (PLA).[27] That all entities involved in PEACE's construction, funding, ownership, and operation

20 Fouquet, "Cut undersea cable, 5.

21 Burdette, "Leveraging submarine cables for political gain."

22 S. Eder, R. Arcesati, and J. Mardell, "Networking the 'Belt and Road': The future is digital," Mercator Institute for China Studies, August 28 2019, https://merics.org/en/tracker/networking-belt-and-road-future-digital.

23 O. Khazan, "The Creepy, Long-Standing Practice of Undersea Cable Tapping," The Atlantic, July 16, 2013, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/

24 Ministry of Foreign Affairs of the People's Republic of China, "Vision and actions on jointly building Belt and Road," full text version, 2015, https://www.mfa.gov.cn/ce/cede/det/zt/yidaiyilude/t1250293.htm.

25 PEACE-MED's cable landings in Cyprus, Abu Talat, Marseille, and Malta were all completed during the course of 2021, while stub branching units have been reserved for direct landing points to other countries, thereby providing additional access options and opportunities for the entire Mediterranean region. PEACE-MED, a 3,200 km cable that connects Egypt to France, went online in March 2022. The cable is slated for completion this year.

26 PeaceCable.net, "PEACE Cable and PCCW Global to leverage Infinera's ICE6 for high-performance PEACE submarine cable," n.d., accessed August 28, 2022, http://www.peacecable.net/News/Detail/16630.

27 J. E. Hillman, *The Digital Silk Road: China's quest to wire the world and win the future* (London: Profile Books, 2021).

are Chinese ensures that Beijing maintains supreme control over this network.[28] Xi himself has outlined the logic underlying this approach: "The control of core technology by others is our biggest hidden danger," and allowing foreigners to control core technology "is like building a house on someone else's foundation."[29] Viewed through this lens, PEACE is not only an economic endeavor but a geostrategic one.

In addition to providing high-speed access to MENA countries, boosting digital connectivity, and stimulating economic growth, China is seeking to simultaneously reduce its dependence on foreign cables while making other countries more dependent on Chinese networks.[30] As more and more nations come to rely on Chinese infrastructure, the asymmetry shifts in Beijing's favor, affording China more leverage and influence in the digital realm and beyond. China can wield this control to favorably shape the physical form of the internet for its own strategic purposes.[31] For a country that has declared its desire to become a "cyber superpower,"[32] the ability to decide when, where, and how to build subsea fiber optics affords China substantial normative power. As Xi explained in reference to telecommunications and cybersecurity, the "game of great powers is not only a game of technology but also a game of ideas and discourse power."[33] Xi's sentiments reveal that China's push to gain increasing control over critical digital infrastructure is crucial in its quest to play a more prominent role in internet governance and promote its vision of cyber sovereignty. Xi's statement also helps to contextualize China's move to designate data as a factor of production, alongside land, labor, and capital: more control over global data flows bolsters China's ability to project discursive power and shape the information environment. Data gleaned from these networks can also be processed to improve goods and services to countries participating in the BRI or for national security purposes.

PEACE also harbors significant value to China because it connects Chinese assets (both civilian and military) across the regions it traverses. The cable, running over land from Kashgar, in the western part of the disputed Xinjiang region, to the port of Gwadar, Pakistan, is a critical link in the BRI's $62 billion China-Pakistan Economic Corridor (CPEC). Yet some observers, such as Pakistan-based Adnan Aamir and his co-authors elsewhere in South and East Asia, paint a less-than-rosy picture of CPEC. In the South Asia Journal, they write: "Nearly eight years after China announced a breathtaking list of development projects in the city . . . none of these have been completed and what investment there has done little to create growth or an economy."[34]

However, the long-term advantages of establishing a presence in the region may be viewed differently by strategists in Beijing. Pakistan awarded China the contract for the construction and operation of the facility back in 2013, and China Overseas Port Holding Company is expanding the facility, building nine new berths. From a geostrategic perspective, Gwadar provides an alternate route to the Strait of Malacca—a critical maritime choke point which is traversed for the vast majority (80 percent) of Chinese trade with the world.[35] The strait is so vital to China that the

28 Notably, most Chinese entities, aside from HMN Tech and PCCW, are state owned enterprises. As Sherman 2021 points out "governments can use that control to undermine Internet security and resilience, and favorably shape the topology of the Internet itself, for their own strategic purposes." At the same time, the complex public-private nexus in China suggests that private companies often serve the Communist Party of China's goals.
J. Sherman, "Cyber defense across the ocean floor: The geopolitics of submarine cable security," Atlantic Council, September 13, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/

29 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表 [The full text of Xi Jinping's speech at the Forum on Cybersecurity and Informatization Work]," speech in Beijing, April 25, 2016, http://www.gov.cn/xinwen/2016-04/25/content_5067705.htm

30 This strategy is being employed across the technology stack.

31 J. Sherman, *Cyber defense across the ocean floor: The geopolitics of submarine cable security*, Atlantic Council, Scowcroft Center for Strategy and Security, September 13, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/.

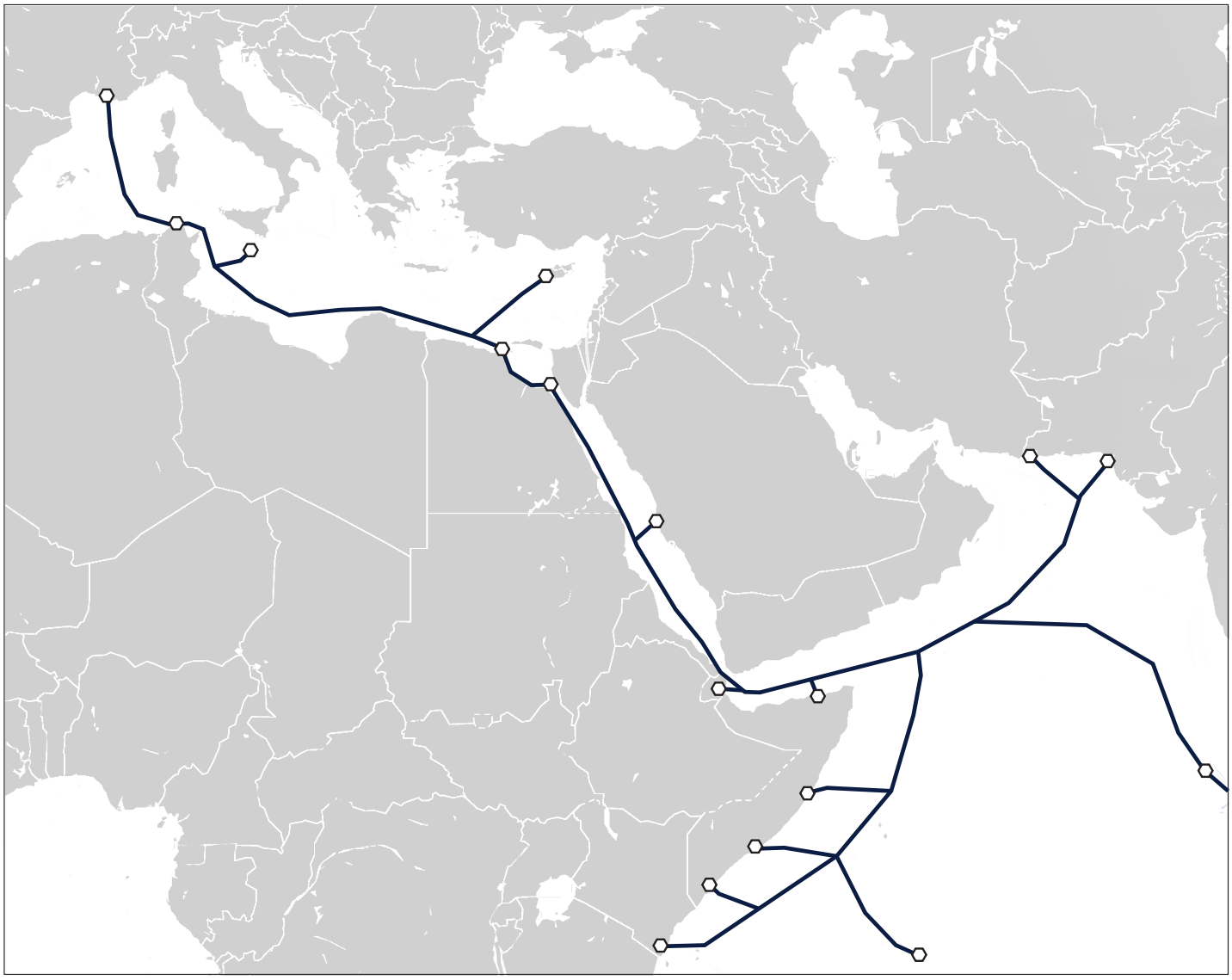
32 Also translated as "network great power."

33 As cited by R. Doshi et al., *China as a "cyber great power": Beijing's two voices in telecommunications*, Brookings Institution, April 2021, https://www.brookings.edu/research/china-as-a-cyber-great-power-beijings-two-voices-in-telecommunications/.

34 A. Aamir et al., "Road to nowhere: China's Belt and Road Initiative at tipping point," *South Asia Journal*, August 11, 2022, http://southasiajournal.net/road-to-nowhere-chinas-belt-and-road-initiative-at-tipping-point/.

35 Marcelo Duhalde et al., "Belt and Road Initiative: China's super link to Gwadar Port—A visual explainer," *South China Morning Post,* n.d., accessed August 29, 2022 https://multimedia.scmp.com/news/china/article/One-Belt-One-Road/pakistan.html.

Figure 2: The PEACE cable connects the Middle East, East Africa, and Europe



Source: "Submarine Cable Map," TeleGeography, is licensed under CC BY-SA 4.0, accessed March 7, 2023, https://www.submarinecablemap.com/.

"Malacca dilemma" is a long-labored question in China's academic and policy debates.[36] Some pundits have speculated that Gwadar could become the site of a PLA Navy and Air Force base. The facility's proximity to the Persian Gulf means that China could use it to support military operations to secure its energy and trade transiting the troubled waters that straddle the MENA region.

The PEACE cable's first stop in North Africa is Djibouti, where the PLA built a naval base in 2016 for $590 million. China's navy has been actively operating in the Gulf of Aden since 2008.[37] Chinese companies have

36 I. Storey, "The Malacca Dilemma: A hindrance to Chinese ambitions in the 21st century," Jamestown Foundation, *China Brief* 6, no. 8 (2006), https://jamestown.org/program/chinas-malacca-dilemma/.

37 E. Lin-Greenberg, "Dragon boats: assessing China's anti-piracy operations in the Gulf of Aden," *Defence & Security Analysis* 26, no. 2 (2010): 213-230, DOI:10.1080/14751798.2010.488867.

since upgraded and expanded the Djibouti port to host aircraft carriers, causing speculation about China's intentions. A future in which Chinese carriers like the newly constructed high-tech *Fujian* are deployed to the region to protect Beijing's regional interests and project power may not be that far away.[38] Additionally, Djibouti port is close to another crucial maritime choke point, the Bab al-Mandab Strait, through which crude oil, condensate, and refined petroleum products were transported in 2018.[39] The PEACE cable then connects Jeddah, Saudi Arabia, to Abu Talat and Zafarana in Egypt before arriving in Europe. Each of these touch points is situated in regions of critical significance to China: a September 2020 report published by Refinitive identified Saudi Arabia as China's second-largest destination for BRI projects in terms of value, with 106 projects valued at $195.7 billion.[40] In Jeddah, specifically, China's COSCO Shipping Ports acquired a 20 percent stake in a terminal located at the Islamic Port.[41] Regarding Egypt, the importance of ensuring the free flow of trade through the Suez Canal was demonstrated vividly in March 2021 when a massive container ship got wedged in the narrow passage, holding up an estimated $9.6 billion of trade along the waterway each day.

China must ensure that all its assets in the region enjoy undisrupted high-speed, low-latency connectivity. Doing so is vital for port operators to optimize and maintain the integrity of supply chains and other activities that ensure the country's continued economic growth.

PEACE in war and espionage

In 2021, cybersecurity company FireEye detected a two-year hacking operation against entities in Israel, the UAE, and Iran that the company claimed was executed by a Chinese espionage group, UNC215. The campaign targeted government institutions, IT providers, and telecommunications firms. FireEye did not implicate the Chinese government. However, the company made sure to point out that the nature of the operation coincides with Beijing's interests.[42] Regardless of whether or not Beijing was directly involved, China's extensive economic interests and growing involvement in MENA affairs elevate the importance of acquiring reliable regional intelligence. Submarine cables could prove useful to China in this regard.

Countries today rely on undersea cables to coordinate most military operations, according to author Jonathan Hillman.[43] And as Bryan Clark, whose work focuses on the future of warfare, points out, "Radiofrequency circuits used by communications satellites have too little bandwidth to accommodate the terabytes of sensor data recorded by various devices, or to fill operational orders needed to support global military operations."[44] The deployment of increasingly sophisticated technology like unmanned vehicles, artificial intelligence, and high-tech aircraft carriers drives further demand for reliable, secure bandwidth. However, because most military communications travel along the same subsea network as civilian and unclassified data, they are susceptible to eavesdropping and disruption. Countries had exploited this vulnerability long before Snowden revealed the US cable-tapping operations: Britain's secret service leveraged the country's control of global telegram cables for intelligence purposes back in the nineteenth

38 In an interview with SupChina, former Australian intelligence analyst Sam Roggeveen pointed out that aircraft carriers "are not war-winning weapons. These are policing weapons, constabulary weapons." As cited by J. Goldkorn, "China's new aircraft carrier and espionage in the internet age—Q&A with former Australian intelligence analyst Sam Roggeveen," SupChina (platform), 2022, https://supchina.com/2022/07/08/chinas-new-aircraft-carrier-and-espionage-in-the-internet-age-qa-with-former-australian-intelligence-analyst-sam-roggeveen/.

39 "The Bab el-Mandeb Strait is a strategic route for oil and natural gas," *Today in Energy* series, US Energy Information Administration, August 27, 2019, https://www.eia.gov/todayinenergy/detail.php?id=41073#:~:text=In percent202018 percent2C percent20an percent20estimated percent206.2,million percent20b percent2Fd percent20in percent202014.

40 Sayed Husein et al., *BRI Connect: An initiative in numbers*, third edition, Refinitive, 2020, https://agsiw.org/wp-content/uploads/2020/02/belt-and-road-initiative-in-numbers-issue-3.pdf.

41 D. Wainwright, "China's Cosco takes 20 percent stake in Saudi container terminal," TradeWinds, DN Media Group, 2021, https://www.tradewindsnews.com/ports/chinas-cosco-takes-20-stake-in-saudi-container-terminal/2-1-960255.

42 L. Tress, "Chinese group carried out widespread cyber espionage campaign in Israel – report," *The Times of Israel*, August 10, 2021, https://www.timesofisrael.com/chinese-group-carried-out-widespread-cyber-espionage-campaign-in-israel-report/

43 Hillman wrote: "The U.S. military has dedicated undersea connections, often called "black fiber." But it still relies on privately owned infrastructure for the vast majority of its communications. See Hillman, *The Digital Silk Road*."

44 B. Clark, "Undersea cables and the future of submarine competition," *Bulletin of the Atomic Scientists* 72, no. 4 (2016): 234-237, https://www.tandfonline.com/doi/full/10.1080/00963402.2016.1195636.

century.[45] The Chinese are scholars of history and understand that expanding the country's stake in the subsea cable sector reduces the ability of others to spy on China while at the same time enhancing Beijing's ability to access sensitive information.

Due to its strategic political-economic importance, the MENA region happens to be an attractive place for cable espionage. Historically, spy agencies such as America's NSA and Britain's Government Communications Headquarters intercepted reams of sensitive data from MENA networks. As Duncan Campbell, an investigative journalist specializing in surveillance since 1975, explained, "there is no question that, in the broadest sense, from Port Said [in Egypt] to Oman is one of the greatest areas for telecommunications traffic and therefore surveillance. Everything about the Middle East goes through that region except for the odd link through Turkey."[46] In Egypt alone, the fifteen cables between the Mediterranean and Red Seas transmit 17 percent to 30 percent of the world's internet traffic—equivalent to the data of 1.3 billion to 2.3 billion people. The ability to intercept data traveling along these networks could provide China with invaluable information. Beijing has expended considerable resources improving intelligence gathering by interception of signals (SIGINT). According to a 2018 estimate, Beijing spent roughly 10 percent of its military budget on enhancing these capabilities.[47] PEACE and other cables built, upgraded, or operated by Chinese companies could prove useful in this regard.

Cable tapping to intercept and decrypt data is a notoriously difficult endeavor.[48] By acquiring stakes in undersea cable networks, companies could help alleviate some of these challenges: installing backdoors during cable manufacturing or construction to siphon data traveling along the network. While firms like Huawei Technologies Co. have repeatedly denied embedding backdoors in their equipment at the central government's behest, Chinese policymakers have been surprisingly open about leveraging such civilian technology for military purposes.[49] In 2016, China Institute of Cyberspace Strategy's director, Qin An, claimed that "due to the highly monopolistic nature of information technology systems, it is unlikely that there will be two different systems for military and civilian use . . . it is particularly necessary [for China] to integrate military and civilian resources through a military-civil fusion system."[50]

Some Chinese firms agreed with Qin's assessment: that same year, one of China's two largest shipbuilders, the China State Shipbuilding Corporation, revealed details of a project known as the underwater great wall: a ship and subsurface sensors' network fitted to fiber-optic cables and landing stations designed to improve its anti-submarine warfare capabilities.[51] While the project is proximate to China's shores, the country has indicated that its subsea monitoring and detection aspirations are global. A year before the conception of the project, a paper issued by China's State Oceanic Administration called for the deployment of undersea observation systems in "the near seas, the depths of the far seas, and around islands bordering the far seas, as well as in strategic passages."[52] Considering that Chinese strategists view it as vital to safeguard "strategic passages" like the Suez Canal-Red Sea-Mandab Strait passage, the extension of such systems to the MENA region makes strategic sense.

45 Headrick, Daniel R., and Pascal Griset. "Submarine telegraph cables: Business and politics, 1838–1939." Business History Review 75, no. 3 (2001): 543-578. https://www.cambridge.org/core/journals/business-history-review/article/abs/submarine-telegraph-cables-business-and-politics-18381939/3C5C58338F96F235DE13BC88B1A45B5D

46 Duncan Campbell as quoted in P. Cochrane, "Red Sea cables: How UK and US spy agencies listen to the Middle East," *Middle East Eye*, March 4, 2021, https://www.middleeasteye.net/news/red-sea-cables-how-us-uk-spy-agencies-listen-middle-east.

47 T. R. McCabe, "Chinese intelligence, surveillance, and reconnaissance systems," *Journal of Indo-Pacific Affairs*, Air University (US Air Force education), March 8, 2021, https://www.airuniversity.af.edu/JIPA/Display/Article/2528263/chinese-intelligence-surveillance-and-reconnaissance-systems/.

48 McCabe, "Chinese intelligence."

49 Z. Hanhau, "Law expert: Chinese government can't force Huawei to make backdoors," *Wired*, 2019, https://www.wired.com/story/law-expert-chinese-government-cant-force-huawei-make-backdoors/.

50 As cited by R. Doshi et al., China as a "cyber great power": Beijing's two voices in telecommunications, Brookings Institution, April 2021, https://www.brookings.edu/research/china-as-a-cyber-great-power-beijings-two-voices-in-telecommunications/.

51 C. Wong, "'Underwater Great Wall': Chinese firm proposes building network of submarine detectors to boost nation's defense," *South China Morning Post*, May 19, 2016, https://www.scmp.com/news/china/diplomacy-defence/article/1947212/underwater-great-wall-chinese-firm-proposes-building.

52 State Oceanic Administration of China, 2015 paper, quoted in Lyle J. Goldstein, "China is building a [sic] 'Undersea Great Wall' to take on America in a war," *National Interest*, October 27, 2019, https://nationalinterest.org/blog/buzz/china-building-undersea-great-wall-take-america-war-90601.

Notably, PEACE cable network's owner, Hengtong Group, has been investing considerable resources into improving China's fiber-optic systems and has established research partnerships with the PLA Naval University of Engineering, Zhongtian Technology Submarine Cable Co. Ltd, and Beijing University of Posts and Telecommunications. Meanwhile, several of Hengtong's subsidiaries have partnered with Chinese universities to develop civilian and military applications for submarine observation networks.[53] The underwater environmental monitoring systems deployed by Chinese companies allow for real-time location and tracing of surface and underwater targets. The systems resemble the US SOSUS network, which employs fixed sensor arrays to detect Russian submarines. Analysts have since noted that these Chinese networks could significantly erode US and Russian undersea warfare superiority and enhance the PLA's ability to project power.

For Israel and the Gulf States, China's relationship with Iran deserves greater scrutiny in this context. In 2021, Beijing and Teheran inked a now infamous quarter-century strategic partnership agreement that includes a commitment to enhancing military cooperation and intelligence sharing. Notably, the deal affords China access to the Iranian port and naval base at Jask, located on the Gulf of Oman.[54] Israel's former chief of military intelligence, Amos Yadlin, commented: "One of the most worrying clauses in the agreement between Iran and China is the intelligence sharing."[55] In a 2021 study published by the Leiden Asia Center, researcher and risk analyst Mohammadbagher Forough highlights that Iran's minister of information and communications technology, Mohammad-Javad Azari Jahromi, has repeatedly called for China and Iran to establish a united *cyber front* against Western hegemony. Forough concludes that "the two countries are not likely to become full 'cyber allies'; however, the strategic partnership is deepening in all fields including cyber."[56] The quarter-century strategic partnership agreement creates a framework for China to share information gleaned from its underwater observation systems with Teheran—complicating and potentially compromising the military operations of Israel and Gulf countries.

There is a caveat regarding leveraging control of subsea cables for espionage in that landing stations are particularly vulnerable to tapping. Therefore, cables landing on their shores could provide MENA countries with monitoring opportunities. Still, the myriad military, intelligence, and geostrategic advantages offered by controlling submarine networks mean that cable networks like PEACE are strategically significant to the Chinese Communist Party, even if not commercially viable. However, it is for these very reasons that fiber optics with Chinese stakeholders have become increasingly embroiled in geopolitics.

PEACE: a flashpoint in the geopolitics of the internet

Like China, other countries understand that protecting the integrity of undersea cable networks is critical to safeguarding economic prosperity and national security. For example, during a 2017 UK parliamentary hearing, then-National Security Adviser Mark Sedwill said attacks on undersea cables may have "the same effect as used to be achieved in, say, World War II by bombing the London docks or taking out a power station." That same year, special assistant to Taiwan's former deputy minister of national defense in Taiwan, Eli Huang, penned an op-ed in *The National Interest* calling the undersea cable network "Taiwan's Achilles' heel in a conflict with China."[57] While concerns surrounding the security of undersea cables are nothing new, the issue of who controls this critical architecture has emerged as a core issue for America and its allies amid rising tensions with China. Within this context, the activity

53 US Senate Committee on Foreign Relations, *The United States and Europe: A concrete agenda for transatlantic cooperation on China, a Majority Report* (Washington: Government Printing Office, 2020), https://www.foreign.senate.gov/imo/media/doc/SFRC percent20Majority percent20China-Europe percent20Report percent20FINAL percent20(P&G).pdf.

54 H. A. Cordesman, "China and Iran: A major Chinese gain in 'white area warfare' in the Gulf," commentary, Center for Strategic and International Studies, March 29, 2021, https://www.csis.org/analysis/china-and-iran-major-chinese-gain-white-area-warfare-gulf.

55 "Ex-IDF intel head: Iran-China megadeal includes 'worrying' military info-sharing," *Times of Israel*, March 29, 2021, https://www.timesofisrael.com/ex-idf-intel-head-iran-china-megadeal-includes-worrying-military-info-sharing/.

56 Mohammadbagher Forough, "Iran and China along the digital Silk Rroad," in *The Digital Silk Road: Perspectives from affected countries*, ed. Rogier Creemers, Leiden Asia Center, July 2021, 24-32, https://leidenasiacentre.nl/wp-content/uploads/2021/08/Digital-Silk-Road-Perspectives-From-Affected-Countries.pdf.

57 E. Huang, "Taiwan's Achilles' heel in a conflict with China is not what you think, *National Interest*, December 3, 2017, https://nationalinterest.org/blog/the-buzz/taiwans-achilles percentE2 percent80 percent99-heel-conflict-china-not-what-you-think-23481.

beneath MENA's waters, particularly PEACE, has not gone unnoticed.

In his book, *The Digital Silk Road: China's quest to wire the world and win the future*, Jonathan Hillman argues that China's growing digital presence in Djibouti, "a critical choke-point in global communications," could compromise America's regional operations.[58] Since authoring the book, Hillman has joined the US State Department as a policy adviser. To illustrate what could happen in the event of a disruption, the author points to the severing of three cables linking Egypt and Italy in 2008, when US drone launches in Iraq dwindled "from hundreds to tens a day." Despite America's declared departure from the Middle East under President Obama, the United States remains an actively engaged security guarantor. Thus, the United States must ensure its assets remain connected, and its communications are not compromised. A September 2020 report by the US Senate Committee on Foreign Relations, titled "The United States and Europe: A concrete agenda for transatlantic cooperation on China," outlined these concerns in detail.[59] Notably, the report dedicates an entire chapter to the issue of undersea cables, with PEACE being the primary case study. The committee declared that the most immediate risk "is to data and cybersecurity, and the use of cables for intelligence gathering." Perhaps ironically, the paper describes America's very own multiyear cable-tapping operations to demonstrate the feasibility of executing cable espionage. Beyond espionage, the report cites Hengtong's close ties to the CCP and the PLA and its involvement in projects that advance China's "civil-military fusion" efforts as cause for concern.

At its core, the current feud over who controls the world's internet infrastructure harbors a structural dimension that relates to the relative decline of American power. Despite China's significant strides into the subsea cable industry, the United States still dominates the market. Roughly a quarter of the world's global data flows today travel via the United States—including 63 percent of international traffic en route to China. As Hillman points out, this dominance has afforded America invaluable economic and military advantages that US intelligence officials have described as a "tremendous home-field advantage."[60] Washington is therefore concerned about Beijing's stated goal of capturing 60 percent of the global fiber-optic communications market by 2025. For a country that is often criticized for being opaque, China has been rather candid about the nature of its expansion in the subsea cable market. According to one official Chinese Communist Party outlet, "although undersea cable laying is a business, it is also a battlefield where information can be obtained."[61] Here, "information" reads "data"—arguably the most significant strategic asset in the twenty-first century. As the fourth industrial revolution gains steam, access to data and the ability to protect its integrity will become increasingly vital to ensuring national security and economic prosperity.

A March 2021 report by Bloomberg identified PEACE as "a new flashpoint in the geopolitics of the internet." Indeed, the dynamics at play suggest that it could emerge as precisely that. America and its allies have not stood idly by as Chinese companies have risen up the technological value chain and captured an increasing share of the market: Canberra effectively blocked a 2016 deal with Huawei Marine to construct a 4,000 km cable connecting Solomon Islands to Sydney amid fears that Huawei's involvement would compromise Australia's network. More recently, the US government intervened to stop the Pacific Light Cable Network from connecting Hong Kong to Los Angelis via a cable measuring 12,800 km. The United States also has fired shots from its economic cannon, imposing trade restrictions on Huawei and Hengtong. In January 2022, the US FCC effectively ejected China Unicom from the US market over security concerns.[62]

The European Union has joined the United States in imposing tariffs on several Chinese entities, including Hengtong, after an investigation revealed that they were unfairly undercutting competition: selling cables to the European market at "artificially low prices." Meanwhile, Google and Meta have already stated they would not utilize PEACE, though the aforementioned

58 Huang, "Taiwan's Achilles' heel," 19.
59 US Senate Committee on Foreign Relations,, The United States and Europe: A concrete agenda for transatlantic cooperation on China, 53.
60 Huang, "Taiwan's Achilles' heel," 19.
61 G. Starks, "Statement of Commissioner Geoffrey Starks," Federal Communications Commission, IB Docket No. 16-155, 2020, https://docs.fcc.gov/public/attachments/DOC-367238A6.pdf.
62 T. Shields, "FCC adds China Unicom to list of Chinese telecoms banned in U.S. on espionage," Bloomberg, January 27, 2022, https://www.bloomberg.com/news/articles/2022-01-27/china-unicom-ejected-from-u-s-as-fcc-cites-security-concerns#xj4y7vzkg.

trade restrictions would make it difficult even if the companies wanted to. Notably, Google and Meta have recently entered the cable market, significantly raising the level of competition. Some have gone as far as to call US tech giants' ambitions to construct and own global data "a tectonic shift in how the internet works and who controls it."[63] These geoeconomic effects are making it harder for China to achieve its goal of dominating the sector.

While PEACE has certainly not eluded the attention of policymakers in Washington, it has thus far not faced any direct pushback from Western powers. Instead, the United States has spent much of its time pressuring countries in the region on 5G (with limited success), neglecting what some have called "the most central part of the global internet infrastructure," and how Beijing is reshaping it. However, US policymakers are increasingly directing their attention to the action on MENA's ocean floor. For example, during an August 2022 Senate Foreign Relations Subcommittee meeting, Senator Bill Hagerty said he is "very concerned about the undersea cables they are laying [in the Middle East] with Chinese systems that make them vulnerable to exploitation."[64] Senator Hagerty, who spent much of his time in his previous position as ambassador to Japan working on removing Huawei from Japanese telecoms networks, singled out PEACE as "a very big concern." When asked by Hagerty what steps the administration is taking to address the PEACE cable, Barbara A. Leaf, assistant secretary of state for Near Eastern affairs, replied: "I am not as well versed, frankly, senator, on this particular technology, dilemma, or threat before us, and I will get myself schooled on it." Senator Hagery suggested that Leaf looks into "the previous administration's work on the SeaMeWe-6 cable", adding that "a tremendous amount of work went into dealing with this exact concern on this undersea cable." The US Trade and Development Agency (USTDA) offered a $3.8 million training grant to five telecom companies in countries on the cable route in return for choosing American SubCom as the supplier over HMN Tech. At the same time, American diplomats warned countries about the potential security risk of involving HMN-Tech equipment and cautioned participating foreign telecom carriers that Washington planned to impose severe sanctions on HMN Tech, a development that could put their investment in the cable project at risk. Ultimately, China Telecom and China Mobile withdrew their combined investment of roughly 20 percent from the $ 500 million SMW 6 project in 2022 after HMN-Tech lost the bid. Notably, China Unicom and PCCW remain involved in the project.

Since at least July 2022, the United States has reoriented its engagement with the MENA region to counter Beijing's growing regional influence. Biden's visit to the region during July-August 2022, which saw Saudi Arabia commit to cooperating with the United States on 5G open radio access network (RAN) technology and Israel ink an agreement to deepen technology cooperation with America, is emblematic of this new approach. These deals also reflect that technology rests at the core of US concerns regarding China. Assistant Secretary Leaf made sure to mention that "more broadly, across the region, we [America] are all over this issue of untrusted vendors in the information communications technology sphere." She added that the United States has been "working across the region to inform, illuminate, and educate host governments on the risks."

The US Department of Defense has come to view the Middle East as "a key theater for competing with China."[65] As tensions between China and the West continue to simmer, PEACE could become the next target in the great power competition between the United States and China. Regardless, with China's share of the cable market set to grow, Middle Eastern countries would do well to direct more attention and resources to ensuring these "vital arteries" of information remain secure. Doing so is both a matter of national security and economic prosperity.

63 A. Blum and C. Baraka, "Sea change," *Rest of World*, May 10, 2022, https://restofworld.org/2022/google-meta-underwater-cables/.

64 *China's Role in the Middle East: Hearing Before the Senate Foreign Relations Subcommittee on Near East, South Asia, Central Asia, and Counterterrorism*, 117th Cong. (2022) (testimony of Barbara A. Leaf, assistant secretary of state for Near Eastern affairs), https://www.foreign.senate.gov/hearings/chinas-role-in-the-middle-east080422.

65 T. M. Cronk, "DOD Continues Mission to Stabilize the Middle East," US Department of Defense, April 5, 2022, https://www.defense.gov/News/News-Stories/Article/Article/2990349/dod-continues-mission-to-stabilize-the-middle-east/

Dale Aluf leads SIGNAL's interdisciplinary research team, developing in-depth knowledge and theories for policy practitioners working in the sphere of Sino-Israeli relations. He has been a visiting fellow at the Intellisia Institute in Guangzhou, China, where he researched China's Belt & Road Initiative, the Digital Silk Road, and social science perspectives on artificial intelligence. His areas of expertise include Chinese foreign policy, China-Middle East relations, the geopolitics of technology, cross-cultural analysis, and political psychology. Aluf's writing and commentary have appeared in *The Diplomat, Asia Times, Jerusalem Post, Calcalist, Ynet, N12, Times of Israel, East Asia Forum, Zawya,* and *Defense Horizon Journal*. Before joining SIGNAL in 2017, he worked as a profiler for eight years in Israel's aviation sector, conducting various security assessments in Africa, Asia, and Europe. While living in South Africa, he received training in cognitive neuropsychology and psychodynamic group analysis. Aluf holds an MSc in Applied Psychology from the University of Liverpool and is a member of the International Society of Political Psychology.

Atlantic Council Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Todd Achilles
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*
List as of March 7, 2023

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org