IAI PAPERS 24 | 04 - FEBRUARY 2024

ISSN 2610-9603 | ISBN 978-88-9368-318-0

Istituto Affari Internazionali

Transatlantic Tech Bridge: Digital Infrastructure and Subsea Cables, a US Perspective

by Julia Tréhu and Megan Roberts

Fondazione Compagnia di San Paolo

ABSTRACT

The importance of digital infrastructure for global communication and connectivity is only growing. Within this varied sector, subsea cables play a central role in ensuring seamless internet traffic globally. What are the US's strategic and economic interests in digital infrastructure, particularly subsea cables? Within the context of larger economic and geopolitical competition, US policy is multifaceted, from aiming to secure the physical security of infrastructure and guarding against espionage and technology leakage, to boosting economic competitiveness and supporting domestic firms. Overall, digital infrastructure, and undersea cables in particular, are a key element of a larger US strategy of outcompeting China. Although evaluations among allies of the relative threat posed by China and Chinese-owned digital infrastructure vary, broadly shared goals of resiliency, security, and increased connectivity mean there are potential areas for deeper EU-US cooperation, including partnerships with third countries, that align with their respective strategic visions and represent a solid base for further transatlantic coordination.

USA | European Union | Transatlantic relations | Digital policy | Digital infrastructures

keywords

ISSN 2610-9603 | ISBN 978-88-9368-318-0

Transatlantic Tech Bridge: Digital Infrastructure and Subsea Cables, a US Perspective

by Julia Tréhu and Megan Roberts*

Introduction

Digital infrastructure – the collection of equipment and systems that connect and power electronic communications and the digital world – is the hardware of digital transformation. Since the first telegraph message travelled across the first (analogue) transatlantic cable in 1856,[1] this infrastructure has come to include data centres which power the cloud, undersea cables and wireless terrestrial and satellite networks. Digital infrastructure represents the backbone of digital systems and is where the physical and digital worlds meet. The importance of digital infrastructure for today's economies and societies is growing nonlinearly. An estimated 600 billion US dollars will be invested in the sector by 2035.[2] For governments worldwide, the achievement of broader social and development goals also increasingly hinges on the deployment, maintenance and dependability of digital infrastructure.

Within this broad sector, undersea cables play a crucial role. More than 99 per cent of international internet traffic passes across four hundred subsea cables, although precise calculations are impossible without data on intercontinental satellite traffic.[3] New subsea cable investments reached 2.2 billion US dollars from 2016 to 2018, with forecasts predicting investments exceeding 10 billion US dollars by

[1] Duncan Geere, "How the First Cable Was Laid Across the Atlantic", in *Wired*, 18 January 2011, https://www.wired.co.uk/article/transatlantic-cables.

[2] Barclay Ballard, "Investment in Digital Infrastructure Shows No Sign of Slowing", in *Infrastructure Investor*, 28 June 2023, https://www.infrastructureinvestor.com/?p=148506.

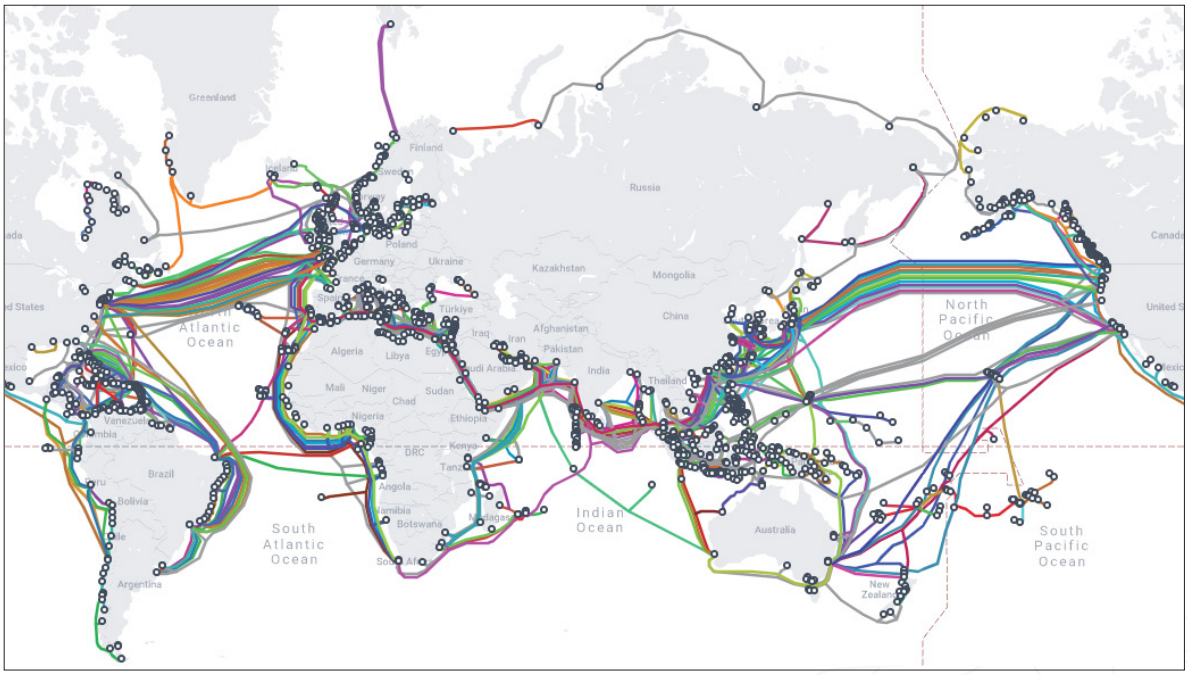
[3] Alan Mauldin, "Do Submarine Cables Account for Over 99% of Intercontinental Data Traffic?", in *TeleGeography Blog*, 4 May 2023, https://blog.telegeography.com/2023-mythbusting-part-3.

* Julia Tréhu is a Paris-based Program Manager and Fellow of the Digital Innovation and Democracy Initiative, German Marshall Fund of the United States. Megan Roberts is former Deputy Director of the Digital Innovation and Democracy Initiative, German Marshall Fund of the United States.

· This paper is part of the project "Building a transatlantic technology bridge: challenges and opportunities", managed by the Istituto Affari Internazionali (IAI), in partnership with the German Marshall Fund of the United States and Centrum für Europäische Politik, and supported by Fondazione Compagnia di San Paolo. An EU perspective on the topic of digital infrastructures is also available as part of the project (see IAI Papers 24|03).

2024.[4] The bodies responsible for laying cable have also evolved over time. The process was initially managed by state-backed companies before being taken over by telecom firms. Today, four "hyperscalers" – Google, Meta, Amazon and Microsoft – are involved in nearly every new cable laid. Along with classic internet traffic, they are focused on the needs related to AI, cloud services and connecting data centres, which drive up data volumes.[5] They work with four major undersea cable firms: the US-based SubCom, the Japanese NEC Corporation, France's Alcatel Submarine Networks and China's HMN Tech.

Figure 1 | Submarine cable map



Source: TeleGeography, *Submarine Cable Map*, last updated 19 January 2024, https://www.submarinecablemap.com.

International communication and the internet as we know it today would not exist without these subsea cables. But the sector is vulnerable to intentional and unintentional disruptions as well as interceptions. These can have massive economic, security and political ramifications. Repair times can also be significant in remote or hard-to-reach locations and repair itself can also introduce vulnerabilities. The first fibre-optic cable was laid in 1988, and the vast majority of internet cables were laid in the post–Cold War era, a manifestation of the globalisation that characterised this period. But these cables also present a new

[4] Natalie Bannerman, "TeleGeography Predicts $10bn Worth of New Subsea Cables by 2024", in *Capacity Media*, 26 April 2022, https://www.capacitymedia.com/article/2a0nvwtoo5r7bm6ab2j28/news/telegeography-predicts-10n-worth-of-new-subsea-cables-by-2024.

[5] Robert Jacques, "Interview: Orange Wholesale Chief Says Hyperscalers, Cloud, AI Fundamentally Changing Subsea Cable", in *TelcoTitans*, 26 October 2023, https://www.telcotitans.com/7371.article.

ISSN 2610-9603 | ISBN 978-88-9368-318-0

domain of tension and competition, with geopolitics descending to the ocean floor. Cable planning and investments are intrinsically tied to political, security and development goals.

This paper analyses strategic interests in digital infrastructure from a US perspective, including challenges and opportunities. It then provides an overview of transatlantic cooperation on digital infrastructure, particularly subsea cables, and identifies areas of further cooperation to achieve shared goals.

1. US strategic interests in digital infrastructure and its industrial policy

The United States' overarching strategic goal is an open, secure, interoperable and global internet, one where US digital leaders can compete (and win). This requires trusted digital infrastructure. US investment in digital infrastructure reveals both domestic and international priorities. The 2021 Bipartisan Infrastructure Bill provides 65 billion US dollars for high-speed internet deployment.[6] Its focus is on providing connectivity for low-income households through the Affordable Connectivity Program and reaching underserved rural, agricultural and tribal areas.[7] The "Internet for All" initiative manages grants for infrastructure and training.[8] In the international development space, digital infrastructure is one of three pillars of USAID's digital strategy and its digital ecosystem framework.[9]

US firms retain a leading position in the ownership of subsea cables, and along with Japanese and French firms continue to supply the equipment for most projects. Cables were traditionally owned by a consortium of telecom firms, but this model has seen its share diminish with the influx of cables owned by content providers (the hyperscalers). Unlike other digital technologies, the supply chain for the raw materials that make up the cables is not dependent on China.[10] Global cooperation takes place through formats like the UN's International Telecommunications Union and multistakeholder arrangements like the International Cable Protection

[6] Amanda Hetler, "Broadband Infrastructure Program Explained: The Details", in *TechTarget*, 12 July 2023, https://www.techtarget.com/whatis/feature/Broadband-infrastructure-program-explained-The-details.

[7] White House, *Fact Sheet: Biden-Harris Administration Celebrates Historic Progress in Rebuilding America Ahead of Two-Year Anniversary of Bipartisan Infrastructure Law*, 9 November 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/09/fact-sheet-biden-harris-administration-celebrates-historic-progress-in-rebuilding-america-ahead-of-two-year-anniversary-of-bipartisan-infrastructure-law.

[8] See the official website: *Internet for All*, https://www.internetforall.gov.

[9] US Agency for International Development (USAID), *Digital Ecosystem Framework* (factsheet), 2022, https://www.usaid.gov/digital-development/digital-ecosystem-framework.

[10] Julia Brackup et al., *Alternative Futures for Digital Infrastructure. Insights and Considerations for the Department of Defense*, Santa Monica, RAND, 2023, p. 20, https://www.rand.org/pubs/research_reports/RRA1859-1.html.

ISSN 2610-9603 | ISBN 978-88-9368-318-0

Committee. The United Nations Convention on the Law of the Sea (UNCLOS) provides an important legal framework for ocean policy and undersea cables, including cable protection zones and a dispute resolution framework. The US, however, has failed to ratify UNCLOS for decades and even in the case of US ratification, credible enforcement would be difficult.[11]

Geopolitics and rising concerns about China have upended the world of subsea cables. Digital infrastructure, and undersea cables in particular, fit into a wider strategy for the US and are a key element of "outcompeting" China. This is leading to what has been dubbed a "subsea cold war".[12] Concerns are multifaceted and overlapping, including the physical security of infrastructure, espionage, economic competitiveness and support for domestic firms, fears of technology leakage and geopolitical competition. In promoting the view that "the digital backbones of the modern economy must be open, trusted, interoperable, reliable, and secure",[13] US strategy is highly focused on countering China's "digital silk road".

Digital infrastructure is critical, but also a potential vector for insecurity and subject to disruptions, both accidental and deliberate. But attribution and assessing conflicting motivations among potential adversaries can be difficult. There is still significant uncertainty around cyberthreats and subsea cables, with limited publicly available information or attribution. The majority of cable faults – around a hundred per year – are attributable to accidental errors, such as damage from fishing vessels, or geologic incidents.[14] But the risk and fear of state-directed cyber-attacks or physical sabotage is rising. Many examples remain hypothetical; and concrete details or attribution are classified or unknown. One of the few known events, a 2022 cyber-attack in Hawaii that the Department of Homeland Security claimed to have foiled, was merely attributed to an "international hacking group".[15] Chinese ships have been accused of damaging cables in the Taiwan straits as part of a pressure campaign on the island.[16]

The US is particularly concerned about potential for espionage from adversaries like China and Russia. Tapping into and filtering the enormous quantities of information on subsea cables is extremely difficult, especially at great depths,

[11] John Kraus, "Unmoored from the UN: The Struggle to Ratify UNCLOS in the United States", in *SAIS Review*, 26 June 2023, https://saisreview.sais.jhu.edu/?p=4774.

[12] Alan Mauldin, *The Subsea Cold War*, presentation at the Submarine Networks World, Singapore, 28 September 2023, https://www2.telegeography.com/hubfs/2023/Presentations/Submarine%20Networks%20World%202023.pdf.

[13] White House, *National Security Strategy*, October 2022, p. 33, https://nssarchive.us/national-security-strategy-2022.

[14] Alan Mauldin, "Cable Breakage: When and How Cables Go Down", in *TeleGeography Blog*, 3 May 2017, https://blog.telegeography.com/what-happens-when-submarine-cables-break.

[15] "Federal Agents Disrupted Cyberattack Targeting Phone, Internet Infrastructure on Oahu", in *Hawaii News Now*, 12 April 2022, https://www.hawaiinewsnow.com/2022/04/13/hsi-agents-honolulu-disrupted-cyberattack-undersea-cable-critical-telecommunications.

[16] Huizhong Wu and Johnson Lai, "Taiwan Suspects Chinese Ships Cut Islands' Internet Cables", in *AP News*, 18 April 2023, https://apnews.com/article/65f10f5f73a346fa788436366d7a7c70.

ISSN 2610-9603 | ISBN 978-88-9368-318-0

and only a few countries likely have such capabilities. Landing stations where cables come ashore, however, have been identified as potential vulnerabilities, where lax security could allow for monitoring or tapping of the cables. The US can illustrate its concerns about growing control of infrastructure by adversaries by pointing to cases like the Federated States of Micronesia, where China pressured the government to grant it control of cables and telecom infrastructure via a Memorandum of Understanding.[17] The point here is that Chinese infrastructure investments through the digital silk road will lead to de-facto control and facilitate espionage. Cost-reduction measures by cable owners have also led to increased deployment of remote network management systems, which introduce new vulnerabilities to hacking or sabotage since they are connected to the internet.[18]

The US has responded to these concerns with legislation like the Secure and Trusted Communications Networks Act of 2019, which charged the Federal Communications Commission with carrying out the complex rip-and-replace process for Huawei-made infrastructure domestically.[19] The US has also expressed concerns about Europe's reliance on 5G infrastructure from Huawei.[20] The National Security Strategy released in October 2022 warns that autocratic governments "leverage access to their markets and control of global digital infrastructure for coercive purposes" and cites China as a source of "untrusted digital infrastructure".[21]

The US has also acted to ensure continued market dominance by US and allied firms. Between 2015 and 2019, Chinese investments through the digital silk road led to control by Huawei Marine (which became HMN Tech in 2019) of about 15 per cent of the global market.[22] Sanctions were placed on HMN Tech in 2021, citing its "intention to acquire American technology to help modernize China's People's Liberation Army".[23] This issue also predates the current Biden Administration. In addition to sanctions placed on Huawei, President Trump's "Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector" provided structure to an interagency team known as "Team Telecom" charged with reviewing foreign

[17] Insikt Group, "The Escalating Global Risk Environment for Submarine Cables", in *Recorded Future*, 27 June 2023, p. 18, https://www.recordedfuture.com/escalating-global-risk-environment-submarine-cables.

[18] Ibid., p. 19.

[19] Cecilia Kang, "'Rip and Replace': The Tech Cold War Is Upending Wireless Carriers", in *The New York Times*, 9 May 2023, https://www.nytimes.com/2023/05/09/technology/cellular-china-us-zte-huawei.html.

[20] Mathieu Pollet and John Hendel, "The West Is on a World Tour Against Huawei", in *Politico*, 28 November 2023, https://www.politico.eu/?p=3926817.

[21] White House, *National Security Strategy*, cit., p. 10.

[22] Anna Gross et al., "How the US Is Pushing China Out of the Internet's Plumbing", in *Financial Times*, 13 June, 2023, https://ig.ft.com/subsea-cables.

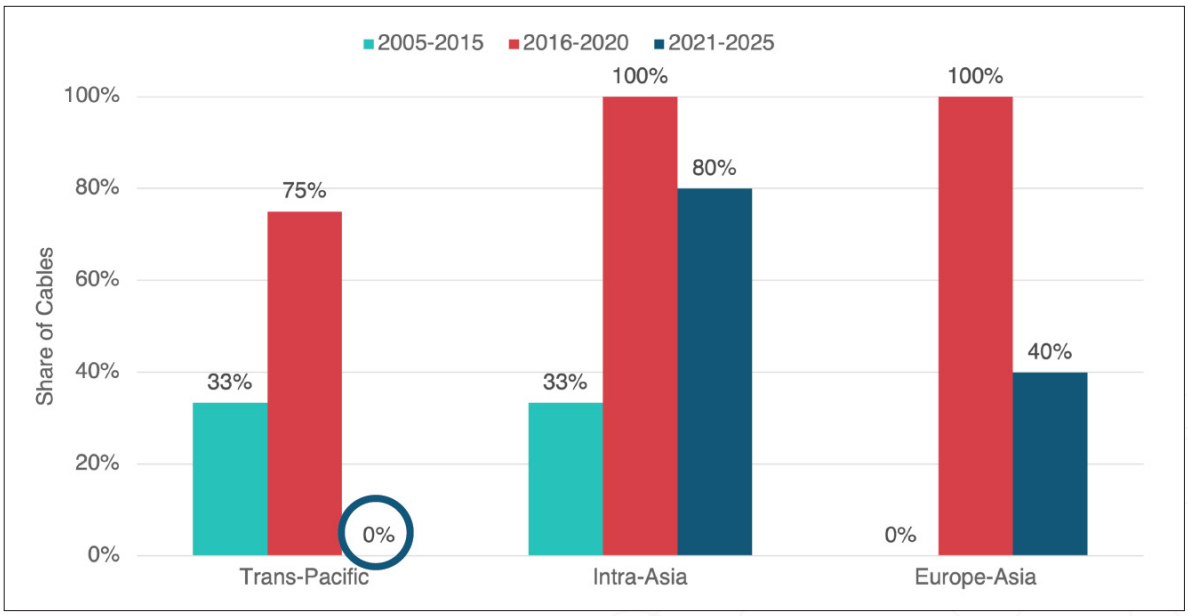
[23] Joe Brock, "U.S. and China Wage War Beneath the Waves: Over Internet Cables", in *Reuters Special Reports*, 24 March 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables.

ISSN 2610-9603 | ISBN 978-88-9368-318-0

investment in telecom and broadcast firms.[24] Run by the Department of Justice's National Security Division, it makes licensing recommendations to the Federal Communications Commission with the goal of ensuring that no cable directly connects the US and the Chinese mainland or Hong Kong.[25] The US Congress has also been somewhat vocal on the issue. For example, the Undersea Cable Control Act passed the House in March 2023.[26]

Recent years have therefore seen significant shifts in undersea cable investment, with many new cables rerouted to avoid China and the South China Sea.[27] While warnings of an undersea splinternet may be exaggerated, the sector is nevertheless seeing important shifts in investment, particularly for transpacific cables. From 2016 to 2020, 75 per cent of cables included at least one Chinese owner. Projections for 2021–2025 plummet to 0 per cent (see Figure 2). Significant reductions are apparent in other Asia connections as well.

Figure 2 | Share of cables entering service with at least one Chinese owner



Notes: Chinese owners include: China Telecom, China Mobile, China Unicom, China Mobile, PCCW, PEACE Cable. Cable year based on RFS.
Source: Alan Mauldin, *The Subsea Cold War*, cit.

[24] White House, Executive Order No. 13913 of 4 April 2020: *Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector*, https://www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states.

[25] Joe Brock, "U.S. and China Wage War Beneath the Waves", cit.

[26] Brian Mast, "Mast Bill to Limit China's Ability to Develop Critical Undersea Cables Passes House", in *Brian Mast Press Releases*, 27 March 2023, https://mast.house.gov/2023/3/mast-bill-to-limit-china-s-ability-to-develop-critical-undersea-cables-passes-house.

[27] Alan Mauldin, *The Subsea Cold War*, cit.

IAI PAPERS 24 | 04 - FEBRUARY 2024 ISSN 2610-9603 | ISBN 978-88-9368-318-0

The US government has also intervened in cases of Chinese involvement in infrastructure projects and exerted pressure which has led to cancellation of cable initiatives or contracts if awarded to Chinese firms. For example, a 2018 proposed consortium led by Amazon, Meta and China Mobile met with opposition from Washington. US security concerns remained even following China Mobile's departure, and the project was shelved despite much of the cable having already been laid.[28] The 600 million US dollar SeaWeMe-6 cable connecting Singapore to France was awarded to the US's SubCom over HMN Tech following diplomatic pressure and incentives like training grants to local telecom firms from the US Trade and Development Agency.[29] At the same time, this pressure, along with sanctions, has influenced cable-building endeavours that do not include US investors or connect geographically to the US.[30]

Such events illustrate the strategic competitive and economic interests at stake, as technology becomes a key site of geopolitical competition. In order to counter China, the United States is working to build a network of partnerships on digital infrastructure. The US CABLES programme provides capacity building and technical assistance to members of the Quad alliance in the Indo-Pacific.[31] The Partnership for Global Infrastructure and Investment (PGII) through the G7 aims to offer an alternative to China's Belt and Road Investments,[32] and included cables as part of a recent PGII announcement on the sidelines of the G20.[33] The US also launched the Trilateral Partnership for Infrastructure Investment with Australia and Japan in 2018.[34] The NATO undersea infrastructure coordination cell, launched in 2023, coordinates between military, civilian and industry interests in subsea infrastructure to increase security.[35] The State Department's 2020 Clean Network Initiative, whose scope extends beyond subsea cables, created a set of shared principles and practices for countries and companies with the goal of blocking Chinese market dominance.[36]

[28] Anna Gross et al., "How the US Is Pushing China Out of the Internet's Plumbing", cit.

[29] Joe Brock, "U.S. and China Wage War Beneath the Waves", cit.

[30] Anna Gross et al., "How the US Is Pushing China Out of the Internet's Plumbing", cit.

[31] White House, *Quad Leaders' Summit Fact Sheet*, 20 May 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet.

[32] White House, *Fact Sheet: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment*, 26 June 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment.

[33] White House, *Fact Sheet: President Biden and Prime Minister Modi Host Leaders on the Partnership for Global Infrastructure and Investment*, 9 September 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/09/fact-sheet-president-biden-and-prime-minister-modi-host-leaders-on-the-partnership-for-global-infrastructure-and-investment.

[34] Mari Yamaguchi, "Japan, Australia, US to Fund Undersea Cable Connection in Micronesia to Counter China's Influence", in *AP News*, 7 June 2023, https://apnews.com/article/155cd017a5a3045bf5078e5df25f17d9.

[35] NATO, *NATO Stands Up Undersea Infrastructure Information Cell*, 15 February 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.

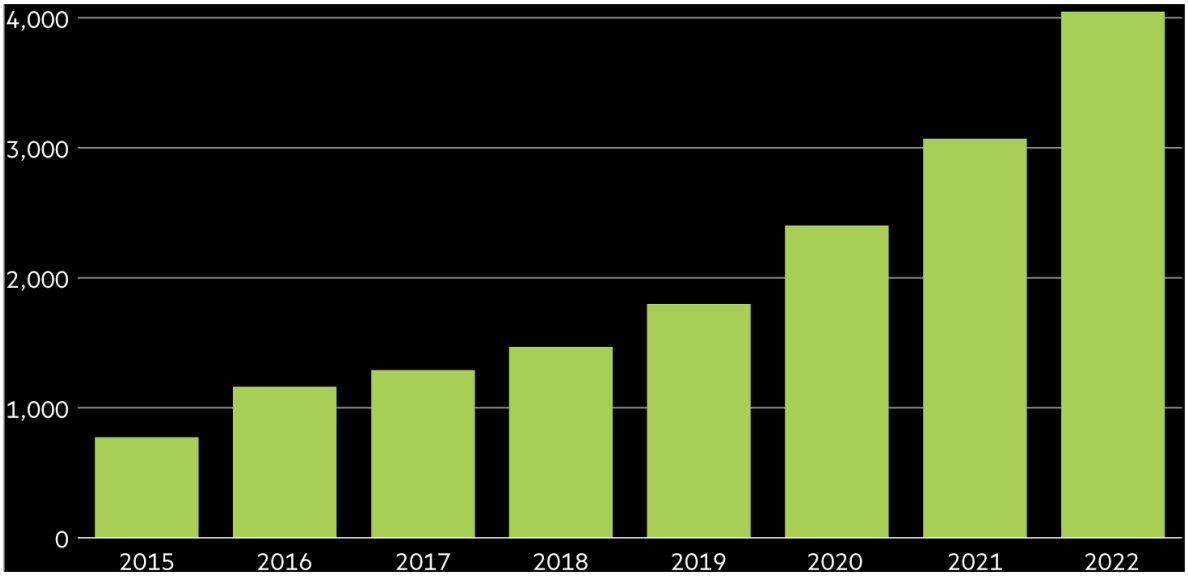
[36] Harvard Business Review, "How the Clean Network Changed the Future of Global Technology Competition", in *Cold Call*, Episode 158 (5 October 2021), https://hbr.org/podcast/2021/10/how-the-

ISSN 2610-9603 | ISBN 978-88-9368-318-0

2. Challenges and opportunities

The US's vision of a global internet runs up against several important challenges. De-risking or decoupling from China or untangling the networks of cables built up through years of collaboration due to security and economic concerns may be easier said than done. Internet traffic often travels on China-owned cables and data continues to flow between the two countries regardless of whether the cable was laid by a US or Chinese supplier.[37]

Figure 3 | Number of directly connected Chinese and US IP network operators



Source: Anna Gross et al., "How the US Is Pushing China Out of the Internet's Plumbing", cit..

China has also been successful in generating digital partnerships worldwide. This digital diplomacy is particularly notable in Africa in financing of digital infrastructure.[38] But among US partners and allies, evaluations of the relative threat posed by China and Chinese-owned digital infrastructure vary.

Many investments in this sector are strictly commercial, and require coordination across a wide range of partners and equities. Almost all global internet traffic, including for public bodies, relies on cable owned by private firms.[39] These private firms can be hesitant about sharing data with public entities via bodies like the

clean-network-changed-the-future-of-global-technology-competition.

[37] Alan Mauldin, *The Subsea Cold War*, cit.

[38] Joseph B. Keller, "The Next Superpower Battlefield Could Be Under the Sea in Africa", in *Foreign Policy*, 10 March 2023, https://foreignpolicy.com/2023/03/10/africa-china-russia-subsea-cables.

[39] Jill C. Gallagher, "Undersea Telecommunication Cables: Technology Overview and Issues for Congress", in *CRS Reports*, 13 September 2022, https://crsreports.congress.gov/product/details?prodcode=R47237.

ISSN 2610-9603 | ISBN 978-88-9368-318-0

Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, founded in 2016.[40]

Amidst these real challenges, however, lie important opportunities. The US hopes to lead and stands to capitalise on the massive boost in investment in digital infrastructure, especially as US-based firms continue to dominate across digital technologies and services generally. Subsea cables are critical for connecting the data centres that power digital advances, including for US tech companies. While these firms' incentives are not always aligned with the US government's strategic concerns, their global success is still part of the US's overall strategy on digital infrastructure, trade and development. Increased investment in cables can also boost cooperation with third countries to increase connectivity in areas with the greatest digital divide, helping integrate them into the global economy and achieve wider development goals.

3. EU-US cooperation

In addition to the global initiatives cited above, the United States and European Union have also cooperated through dedicated venues. The EU-US Trade and Technology Council (TTC) has been an important forum for coordination on digital infrastructure and subsea cables to meet shared goals. The evolution of language from the official TTC statements shows increasing focus on the issue. Of the ten working groups announced following the first meeting in September 2021 in Pittsburgh, Working Group 4 on information and communications technology (ICT) security and competitiveness was tasked with "ensuring security, diversity, interoperability and resilience across the ICT supply chain", finding avenues for joint public financing for secure and resilient digital infrastructure in third countries, and ensuring cooperation on 5G and 6G systems and beyond.[41] A dedicated taskforce on the issue was launched following the second meeting in May 2022 in Saclay, France. This led to the announcement in December 2022 of joint efforts on secure digital connectivity with Jamaica and Kenya, followed by further partnerships with Costa Rica and the Philippines announced in Luleå, Sweden in May 2023. The December 2022 statement references the 'intended focus on subsea cable connectivity and security, the development of alternate routes connecting Europe, Asia and North America, and supplier diversification efforts of Working Group 4 on ICT security and competitiveness.[42] The May 2023 TTC statement included aims to "advance cooperation to promote the selection of trusted subsea

[40] US Department of Homeland Security-Office of Inspector General, "DHS Made Limited Progress to Improve Information Sharing Under the Cybersecurity Act in Calendar Years 2017 and 2018", in *OIG Reports*, 25 September 2020, https://www.oig.dhs.gov/node/6120.

[41] European Commission website: *Working Group 4: ICT Security and Competitiveness*, https://futurium.ec.europa.eu/en/group/65.

[42] EU-US Trade and Technology Council, *EU-US Joint Statement of the Trade and Technology Council*, 5 December 2022, https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7516.

ISSN 2610-9603 | ISBN 978-88-9368-318-0

cable providers for new cable projects – in particular for intercontinental ICT cable projects that promote trustworthy suppliers, reduce latency and enhance route diversity" and the intent to "continue discussions on ensuring transatlantic subsea cables' connectivity and security, including on alternate routes that connect Europe, North America and Asia".[43]

This language mirrors that of the 2023 G7 Leaders communique, which underlined shared goals of "cooperation within the G7 and with like-minded partners to support and enhance network resilience by measures such as extending secure routes of submarine cables" including "supplier diversification efforts in ICTS supply chains" and further discussion of "market trends towards open, interoperable approaches, alongside secure, resilient and established architecture in a technology neutral way".[44]

Geopolitical tensions and attempts to avoid Chinese suppliers have led to cooperation on new routes and cable development. Tensions with Russia, for example, led to the scrapping of a proposed cable running along the Russian Arctic coastline. Instead, the first Artic cable will connect the Nordic countries to Greenland, Canada and Alaska, ending in Japan, and involve a consortium of Finnish, American and Japanese firms.[45] This type of project also illustrates attempts to chart new routes as climate change affects the calculus of laying cable through the Arctic.[46]

The EU and US, however, do not completely see eye to eye on this issue. Some EU member states have shown more willingness to working with Chinese suppliers. The 2022 Peace cable connecting France to Pakistan via Kenya, for example, was entirely financed and built by Chinese firms.[47] While the EU and US have managed to identify third countries with which to cooperate, they hold different perspectives on the relative value of specific projects and different risk perceptions regarding suppliers. The future of the TTC is also in question. The planned December 2023 meeting was postponed until January 2024, with a potentially final TTC to be held in April 2024, and the political will required to sustain the pace of such an initiative

[43] EU-US Trade and Technology Council, *Joint Statement EU-US Trade and Technology Council of 31 May 2023 in Lulea, Sweden*, https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992.

[44] G7, *G7 Hiroshima Leaders' Communiqué*, 20 May 2023, point 39, http://www.g7.utoronto.ca/summit/2023hiroshima/230520-communique.html.

[45] Anne Kauranen, "Arctic Data Cable Linking Europe to Japan Secures First Investment", in *Reuters*, 2 December 2022, https://www.reuters.com/technology/arctic-data-cable-linking-europe-japan-secures-first-investment-2022-12-02.

[46] Isabelle Bousquette, "What Will It Take to Connect the Arctic? $1.2 Billion, 10,000 Miles of Fiber-Optic Cable, and Patience", in *The Wall Street Journal*, 10 March 2023, https://www.wsj.com/articles/what-will-it-take-to-connect-the-arctic-1-2-billion-10-000-miles-of-fiber-optic-cable-and-patience-2af75543.

[47] Anne Cagan, "Entre les Etats-Unis et la Chine, l'âpre bataille des câbles sous-marins", in *L'Express*, 28 September 2022, https://www.lexpress.fr/economie/high-tech/entre-les-etats-unis-et-la-chine-l-apre-bataille-des-cables-sous-marins_2180913.html.

ISSN 2610-9603 | ISBN 978-88-9368-318-0

may be in short supply in a year of EU Parliamentary and US Presidential elections.

4. Future prospects for EU-US cooperation

The importance of digital infrastructure and broadly shared goals of resiliency and increased connectivity mean there are potential areas for deeper EU-US cooperation that align with their respective strategic visions. The following are suggestions for possible collaboration and alignment:

1. *The EU and US should build on the TTC's achievements to date and strengthen digital diplomacy*. Existing cooperation to expand digital cable infrastructure should be strengthened, either within or outside the TTC. Partnerships can continue to be built with individual countries, including third-country partnership opportunities. In some cases, these partnerships will overlap with broader development goals, helping increase connectivity in Global South countries. In others, partnerships will help respond to security concerns, and increase redundancy across networks to increase overall resiliency. Digital capacity-building efforts can be tied to efforts to increase the security of digital infrastructure, and this foundation can be used to build a shared assessment of trusted providers.

2. *There is a need to boost information sharing and coordinated planning related to subsea cables*, both for the transatlantic partnership and with a larger group of like-minded countries. This includes greater understanding of possible cyber-threats, and new vulnerabilities tied to the changing nature of cable deployment and management. Doing so will require balancing sometimes competing concerns from government, with a focus on cybersecurity and geopolitical risks, and industry, whose threat perception is more focused on physical disruptions. Coordination requires input from the broader group of stakeholders, from the various firms qualified as industry (manufacturers, small and large cable or telecom firms, and hyperscalers) and local, state and federal governments. This coordination should also include contingency planning for major disruptions. Shared information can itself serve as a deterrent for malicious attacks.[48] Overall, coordination will ensure that efforts to combat threats do not harm overall connectivity by ensuring various stakeholders are not inadvertently working at cross-purposes.

3. *The EU and US should coordinate and deepen investment in global cooperation formats* like the International Telecommunications Union and multistakeholder arrangements like the International Cable Protection Committee (ICPC) to improve resilience and security. Greater coordination in the ICPC, in particular, would have the benefit of strengthening ties with its private-sector members.[49] Greater buy-in

[48] See Kevin Frazier, "Policy Proposals for the United States to Protect the Undersea Cable System", in *Case Western Reserve Journal of Law, Technology & the Internet*, Vol. 13, No. 1 (2022), https://scholarlycommons.law.case.edu/jolti/vol13/iss1/1.

[49] See ICPC website: https://www.iscpc.org.

IAI PAPERS 24 | 04 - FEBRUARY 2024 ISSN 2610-9603 | ISBN 978-88-9368-318-0

from all members can help augment the above-mentioned recommendations on third-country cooperation and the information-sharing necessary to set clearer standards for security, including cable-laying and repair. Existing frameworks such as the 2020 recommendation on the governance of infrastructure from the Organisation for Economic Cooperation and Development can help guide this coordination.[50] Best practices agreed through these existing multistakeholder arrangements can help guide the coordination initiatives recommended above and serve as a central repository for information and expertise.

4. *There is an opportunity to close holes in both domestic and international legal frameworks governing subsea cables*. US government authority is relatively fractured across agencies, and UNCLOS is unlikely to be ratified anytime soon (if ever). Cables can be owned by multiple entities subject to different jurisdictions. Legal scholars continue to debate the unresolved issue of international law as it pertains to the protection of subsea cables, especially in wartime, as cables could be classified as serving both civilian and military objectives, opening up potential status as legitimate targets. An international treaty should serve as the ultimate goal. But in the meantime, further efforts to provide joint explanations of understanding of international law related to subsea cables could serve as a building block for closing these holes.

5. *As cable infrastructure expands rapidly, physical threats also multiply, and will require new understanding and approaches in order to ensure network resiliency*. Transatlantic joint funding and coordination with third countries could help expand understanding of underwater seismic activity, tsunami and other natural disasters that can affect the undersea cable infrastructure. The accelerating climate crisis heightens the importance of areas that are both susceptible to natural disasters and geopolitically important.[51] There is potential for increased cooperation with countries with highest risk of natural disasters to ensure security of critical infrastructure. Existing or new third-country ICT partnerships should make sure to account for climate risks and can tie cable security into broader mitigation efforts.

6. Finally, *joint research initiatives should advance investigation into possible or speculative future use cases*, such as power-over-fibre.[52] Another possible avenue for joint research includes quantum-safe encryption algorithms. While optical layer encryption or VPNs can secure data traveling over cables and protect against possible interception or espionage, decryption via quantum computing represents

[50] OECD, *OECD Recommendation on the Governance of Infrastructure*, 17 July 2020, https://www.oecd.org/gov/infrastructure-governance/recommendation.

[51] See Garrett Hinck, "Cutting the Cord: The Legal Regime Protecting Undersea Cables", in *Lawfare*, 21 November 2017, https://www.lawfaremedia.org/article/cutting-cord-legal-regime-protecting-undersea-cables.

[52] Bruce M. Howe et al., "SMART Subsea Cables for Observing the Earth and Ocean, Mitigating Environmental Hazards, and Supporting the Blue Economy", in *Frontiers in Earth Science*, Vol. 9 (March 2022), Article 775544, https://doi.org/10.3389/feart.2021.775544.

ISSN 2610-9603 | ISBN 978-88-9368-318-0

a possible future risk. The National Institute of Standards and Technology is working on post-quantum (quantum-resistant) cryptography standards, which will likely become the global benchmark, but should further involve European researchers, many of whom are leaders in the field.[53] Overall, the EU and US should ensure that their research communities can coordinate on new pathbreaking technologies, including ensuring security and reliability from the start.[54]

While today's global communications may appear fast, seamless and intangible, their reliance on hardware and infrastructure, especially subsea cables, and the physical vulnerabilities they pose and geopolitical tensions they stoke, should never be underestimated. While the EU and US continue to cooperate and largely lead in subsea cables, further cooperation can help fill the gaps. This is crucial to assuage growing security concerns, including guarding against espionage. Cooperation can also help meet shared development goals by partnering with third countries to improve cable access to underserved areas. Although differences remain, shared interest in resiliency and security are a solid base for further transatlantic coordination.

Updated 26 February 2024

ISSN 2610-9603 | ISBN 978-88-9368-318-0

[53] Utilities One, *Understanding Power Transmission in Fiber Optic and Copper Cables*, 15 September 2023, https://utilitiesone.com/understanding-power-transmission-in-fiber-optic-and-copper-cables.

[54] Alina Clasen, "EU Quantum Researchers Set to Give Up IP Rights in Standard-Setting Race", in *Euractiv*, 11 January 2024, https://www.euractiv.com/?p=2031909.

References

Barclay Ballard, "Investment in Digital Infrastructure Shows No Sign of Slowing", in *Infrastructure Investor*, 28 June 2023, https://www.infrastructureinvestor.com/?p=148506

Natalie Bannerman, "TeleGeography Predicts $10bn Worth of New Subsea Cables by 2024", in *Capacity Media*, 26 April 2022, https://www.capacitymedia.com/article/2a0nvwtoo5r7bm6ab2j28/news/telegeography-predicts-10n-worth-of-new-subsea-cables-by-2024

Isabelle Bousquette, "What Will It Take to Connect the Arctic? $1.2 Billion, 10,000 Miles of Fiber-Optic Cable, and Patience", in *The Wall Street Journal*, 10 March 2023, https://www.wsj.com/articles/what-will-it-take-to-connect-the-arctic-1-2-billion-10-000-miles-of-fiber-optic-cable-and-patience-2af75543

Julia Brackup et al., *Alternative Futures for Digital Infrastructure. Insights and Considerations for the Department of Defense*, Santa Monica, RAND, 2023, https://www.rand.org/pubs/research_reports/RRA1859-1.html

Joe Brock, "U.S. and China Wage War Beneath the Waves: Over Internet Cables", in *Reuters Special Reports*, 24 March 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables

Anne Cagan, "Entre les Etats-Unis et la Chine, l'âpre bataille des câbles sous-marins", in *L'Express*, 28 September 2022, https://www.lexpress.fr/economie/high-tech/entre-les-etats-unis-et-la-chine-l-apre-bataille-des-cables-sous-marins_2180913.html

Alina Clasen, "EU Quantum Researchers Set to Give Up IP Rights in Standard-Setting Race", in *Euractiv*, 11 January 2024, https://www.euractiv.com/?p=2031909

EU-US Trade and Technology Council, *EU-US Joint Statement of the Trade and Technology Council*, 5 December 2022, https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7516

EU-US Trade and Technology Council, *Joint Statement EU-US Trade and Technology Council of 31 May 2023 in Lulea, Sweden*, https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992

Kevin Frazier, "Policy Proposals for the United States to Protect the Undersea Cable System", in *Case Western Reserve Journal of Law, Technology & the Internet*, Vol. 13, No. 1 (2022), https://scholarlycommons.law.case.edu/jolti/vol13/iss1/1

G7, *G7 Hiroshima Leaders' Communiqué*, 20 May 2023, http://www.g7.utoronto.ca/summit/2023hiroshima/230520-communique.html

ISSN 2610-9603 | ISBN 978-88-9368-318-0

Jill C. Gallagher, "Undersea Telecommunication Cables: Technology Overview and Issues for Congress", in *CRS Reports*, 13 September 2022, https://crsreports.congress.gov/product/details?prodcode=R47237

Duncan Geere, "How the First Cable Was Laid Across the Atlantic", in *Wired*, 18 January 2011, https://www.wired.co.uk/article/transatlantic-cables

Anna Gross et al., "How the US Is Pushing China Out of the Internet's Plumbing", in *Financial Times*, 13 June, 2023, https://ig.ft.com/subsea-cables

Harvard Business Review, "How the Clean Network Changed the Future of Global Technology Competition", in *Cold Call*, Episode 158 (5 October 2021), https://hbr.org/podcast/2021/10/how-the-clean-network-changed-the-future-of-global-technology-competition

Amanda Hetler, "Broadband Infrastructure Program Explained: The Details", in *TechTarget*, 12 July 2023, https://www.techtarget.com/whatis/feature/Broadband-infrastructure-program-explained-The-details

Garrett Hinck, "Cutting the Cord: The Legal Regime Protecting Undersea Cables", in *Lawfare*, 21 November 2017, https://www.lawfaremedia.org/article/cutting-cord-legal-regime-protecting-undersea-cables

Bruce M. Howe et al., "SMART Subsea Cables for Observing the Earth and Ocean, Mitigating Environmental Hazards, and Supporting the Blue Economy", in *Frontiers in Earth Science*, Vol. 9 (March 2022), Article 775544, https://doi.org/10.3389/feart.2021.775544

Insikt Group, "The Escalating Global Risk Environment for Submarine Cables", in *Recorded Future*, 27 June 2023, https://www.recordedfuture.com/escalating-global-risk-environment-submarine-cables

Robert Jacques, "Interview: Orange Wholesale Chief Says Hyperscalers, Cloud, AI Fundamentally Changing Subsea Cable", in *TelcoTitans*, 26 October 2023, https://www.telcotitans.com/7371.article

Cecilia Kang, "'Rip and Replace': The Tech Cold War Is Upending Wireless Carriers", in *The New York Times*, 9 May 2023, https://www.nytimes.com/2023/05/09/technology/cellular-china-us-zte-huawei.html

Anne Kauranen, "Arctic Data Cable Linking Europe to Japan Secures First Investment", in *Reuters*, 2 December 2022, https://www.reuters.com/technology/arctic-data-cable-linking-europe-japan-secures-first-investment-2022-12-02

Joseph B. Keller, "The Next Superpower Battlefield Could Be Under the Sea in Africa", in *Foreign Policy*, 10 March 2023, https://foreignpolicy.com/2023/03/10/

ISSN 2610-9603 | ISBN 978-88-9368-318-0

africa-china-russia-subsea-cables

John Kraus, "Unmoored from the UN: The Struggle to Ratify UNCLOS in the United States", in *SAIS Review*, 26 June 2023, https://saisreview.sais.jhu.edu/?p=4774

Brian Mast, "Mast Bill to Limit China's Ability to Develop Critical Undersea Cables Passes House", in *Brian Mast Press Releases*, 27 March 2023, https://mast.house.gov/2023/3/mast-bill-to-limit-china-s-ability-to-develop-critical-undersea-cables-passes-house

Alan Mauldin, "Cable Breakage: When and How Cables Go Down", in *TeleGeography Blog*, 3 May 2017, https://blog.telegeography.com/what-happens-when-submarine-cables-break

Alan Mauldin, "Do Submarine Cables Account for Over 99% of Intercontinental Data Traffic?", in *TeleGeography Blog*, 4 May 2023, https://blog.telegeography.com/2023-mythbusting-part-3

Alan Mauldin, *The Subsea Cold War*, presentation at the Submarine Networks World, Singapore, 28 September 2023, https://www2.telegeography.com/hubfs/2023/Presentations/Submarine%20Networks%20World%202023.pdf

NATO, *NATO Stands Up Undersea Infrastructure Information Cell*, 15 February 2023, https://www.nato.int/cps/en/natohq/news_211919.htm

OECD, *OECD Recommendation on the Governance of Infrastructure*, 17 July 2020, https://www.oecd.org/gov/infrastructure-governance/recommendation

Mathieu Pollet and John Hendel, "The West Is on a World Tour Against Huawei", in *Politico*, 28 November 2023, https://www.politico.eu/?p=3926817

US Agency for International Development (USAID), *Digital Ecosystem Framework* (factsheet), 2022, https://www.usaid.gov/digital-development/digital-ecosystem-framework

US Department of Homeland Security-Office of Inspector General, "DHS Made Limited Progress to Improve Information Sharing Under the Cybersecurity Act in Calendar Years 2017 and 2018", in *OIG Reports*, 25 September 2020, https://www.oig.dhs.gov/node/6120

Utilities One, *Understanding Power Transmission in Fiber Optic and Copper Cables*, 15 September 2023, https://utilitiesone.com/understanding-power-transmission-in-fiber-optic-and-copper-cables

White House, Executive Order No. 13913 of 4 April 2020: *Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector*, https://www.federalregister.gov/

ISSN 2610-9603 | ISBN 978-88-9368-318-0

documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states

White House, *Fact Sheet: Biden-Harris Administration Celebrates Historic Progress in Rebuilding America Ahead of Two-Year Anniversary of Bipartisan Infrastructure Law*, 9 November 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/09/fact-sheet-biden-harris-administration-celebrates-historic-progress-in-rebuilding-america-ahead-of-two-year-anniversary-of-bipartisan-infrastructure-law

White House, *Fact Sheet: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment*, 26 June 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment

White House, *Fact Sheet: President Biden and Prime Minister Modi Host Leaders on the Partnership for Global Infrastructure and Investment*, 9 September 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/09/fact-sheet-president-biden-and-prime-minister-modi-host-leaders-on-the-partnership-for-global-infrastructure-and-investment

White House, *National Security Strategy*, October 2022, https://nssarchive.us/national-security-strategy-2022

White House, *Quad Leaders' Summit Fact Sheet*, 20 May 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet

Huizhong Wu and Johnson Lai, "Taiwan Suspects Chinese Ships Cut Islands' Internet Cables", in *AP News*, 18 April 2023, https://apnews.com/article/65f10f5f73a346fa788436366d7a7c70

Mari Yamaguchi, "Japan, Australia, US to Fund Undersea Cable Connection in Micronesia to Counter China's Influence", in *AP News*, 7 June 2023, https://apnews.com/article/155cd017a5a3045bf5078e5df25f17d9

ISSN 2610-9603 | ISBN 978-88-9368-318-0

ISSN 2610-9603 | ISBN 978-88-9368-318-0

IAI PAPERS 24 | 04 - FEBRUARY 2024

Istituto Affari Internazionali (IAI)
The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17 - I-00186 Rome, Italy
T +39 06 6976831
iai@iai.it
www.iai.it

Latest IAI PAPERS

Director: Riccardo Alcaro (r.alcaro@iai.it)