Luiss
School of Government

Submarine Networks: the backbone of digital ecosystems worldwide and strategic issues

Working Paper Series
SOG-WP3/2024

Authors: Alessandra Galassi, Gianmarco Gabriele Marchionna
May 2024

LUISS

Table of Contents

Abstract

In contemporary times, the arena of geopolitical and geo-economic competition has shifted to the digital realm, where governments and private entities vie for geo-technological supremacy and control of the global order. We are witnessing an escalating installation of submarine fibre-optic cable networks facilitating global connectivity, by carrying all types of data. Interruption of some of these cables would degrade telecom, while disruption of all cables would cease the global Internet. The proprietary structure, trans-jurisdictional nature, and susceptibility to threats make submarine cables pivotal in (cyber-)security challenges. Given their status as critical infrastructure, they deserve to be prioritized in geo-policy debates. This paper undertakes an assessment of strategic, political, economic, and geographical implications of submarine cables, considering them as a power leverage. It explores ongoing initiatives in which Italy actively participates, such as the activation of Sparkle's BlueMed service and the creation of a digital corridor linking the Mediterranean to the Indo-Pacific. We conclude by advocating for proactive collaboration in both country-to-country and country-to-company relations, to ensure responsible functioning of cables. This approach is imperative due to the far-reaching social effects associated with these infrastructures.

Keywords: Submarine Cables, Digital Geopolitics, Geo-Economy, Security, Critical Infrastructure

1. Introduction

While roads or bridges have a visible presence, submarine (or undersea or subsea) cables (SCs) are different: they lie beneath the surface and suffer from invisibility, yet they play a crucial role in the economy and public life of today and decades to come.[1] Not surprisingly, in recent years, major players such as the US, China, and Russia, as well as Big Tech, have paid increasing attention to the strategic importance of the SCs network in the ongoing digital competition for the Great Power.[2] As of June 2023, there exist 485 SCs in operation worldwide, with another 70 planned, that carry more than 97% of all Internet traffic between countries and continents;[3] see Figure 1.

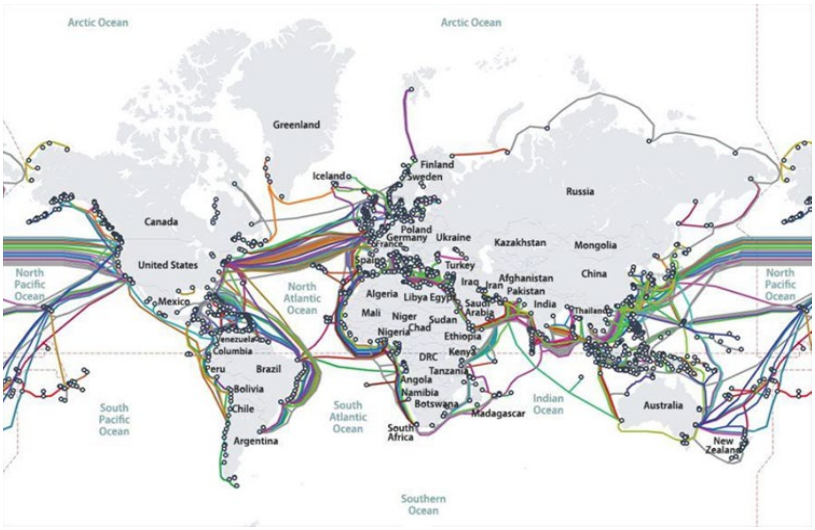

Figure. 1 – Global SCs map between world regions (Source: TeleGeography).

These cables enable society to function in the digital age and have been described by the UN as a "***critical communications infrastructure***" and "***vitally important to the global economy and the***

[1] Beckman, Robert. "Protecting submarine cables from intentional damage—The security Gap." ***Submarine Cables***. Brill Nijhoff (2014). 281-297; see also Clark, Bryan. "Undersea cables and the future of submarine competition." ***Bulletin of the Atomic Scientists*** 72.4 (2016): 234-237; and Starosielski, Nicole. "Warning: do not dig': negotiating the visibility of critical infrastructures." ***Journal of Visual Culture*** 11.1 (2012): 38-57.

[2] Bueger, Christian, and Liebetrau, Tobias. "Protecting hidden infrastructure: The security politics of the global submarine data cable network." ***Contemporary Security Policy*** 42.3 (2021): 391-413.

[3] Davenport, Tara. "Submarine cables, cybersecurity and international law: An intersectional analysis." ***Cath. UJL & Tech*** 24 (2015): 57.

national security of all States."[4] The global cables network spans some 1.4 million kilometres and operates as the "***backbone of the international telecom system***."[5] Consequently, SCs empower daily e-commerce and scientific research, social media posts, banking services, e-mail and video calls - goods we take for granted today - as well as communications of governments and militaries worldwide.[6] The power competition for geo-technological supremacy is thus played out at the submarine level. As a result, SCs are a subject of interest in security studies and global governance. Their interception and disruption pose significant threats, especially in a landscape characterized by ICT dependencies, supply chain vulnerabilities, and widespread reliance on them by all.[7] Hence, increasing risks to cable security and resilience - including from companies' poor security decisions and authoritarian governments' influence-projection - demand stronger cooperation on protecting the Internet along the ocean floor.[8] Consequently, the protection of this infrastructure is becoming one of the most pressing concerns in 21st century for international politics.

SCs are important geopolitically because physically unite two or more countries, strengthening their economic ties, bilateral transactions, data exchange, and political and strategic ties as well. For example, China's approach to Internet as a continuum of national territory could be seen by some observers as a legitimate choice to control information that would otherwise jeopardize national security. However, the Chinese perspective does not fit with the values and cultural context of the EU, where data protection is considered a cornerstone of privacy and is seen as a human right. According to Sherman "***Beijing has long focused on controlling Internet infrastructure at home, nationalizing China's Internet backbone in the 1990s, and might be doing so abroad through its Belt and Road Initiative (BRI).***"[9]

China and the US are the major players and competitors in the digital SCs market. Unlike the US (e.g., AT&T Inc), China has recently begun to invest in infrastructure under the oceans, thanks to the Chinese government strategy dating back to President Xi Jinping's launch of the Digital Silk Road.[10] Moreover, Made in China 2025 plan expresses Beijing's desire to come to own at least 60% of the global fibre-optic market by 2025, shaping the Internet set-up in its favour: more Chinese-funded cables could contribute to greater foreign dependence on China, and more traffic crossing Chinese borders increases the risk of Beijing spying on data.[11] The growing presence of China's State-owned enterprises (SOEs) in the digital SCs market has forced Europe and the US to re-examine the potential and risks of this infrastructure in a new light, raising concerns about the security of data flowing through cables managed by Chinese-invested consortia.[12] It also raised concerns about the ownership structure of these submarine networks and the relationship between owners and cable operators. In fact, Chinese SOEs, through ad-hoc built consortia, maybe both owners and operators of the digital infrastructure and could redirect the flow of data along the cable just as the Chinese government could ask Chinese SOEs to steal data transmitted

[4] Assembly, UN General. "Oceans and the Law of the Sea." ***Report of the Secretary General A/65/37*** (2010).
[5] Assembly, UN General. "Oceans and the Law of the Sea." ***Report of the Secretary General A/70/74*** (2015).
[6] Brake, Doug. "Submarine cables: Critical infrastructure for global communications." ***Information Technology & Innovation Foundation: Washington, DC, USA*** (2019).
[7] Assembly, UN General. "Oceans and the Law of the Sea." ***Report of the Secretary General A/75/340*** (2020).
[8] Hantover, Lixian Loong. "The cloud and the deep sea: How cloud storage raises the stakes for undersea cable security and liability." ***Ocean & Coastal LJ*** 19 (2013): 1.
[9] Sherman, Justin. "Internet security under the ocean: EU-US must cooperate on submarine cable security," ***Italian Institute for International Political Studies: ISPI*** (2022), ***https://www.ispionline.it/en/publication/internet-security-under-ocean-eu-us-must-cooperate-submarine-cable-security-35471***
[10] Shen, Hong. "Building a digital silk road? Situating the internet in China's belt and road initiative." ***International Journal of Communication*** 12 (2018): 19.
[11] Devonshire-Ellis, Chris. "China's Submarine Digital Fiber Optic Belt and Road." ***Silk Road Briefing*** (2022).
[12] Colombo, Matteo. "Network Effects: Europe's Digital Sovereignty in the Mediterranean." ***JSTOR Security Studies Collection*** (2021).

for commercial or military purposes. This security concern has led to the stalling of some projects, such as the HKA (Hong Kong-America) SC after Meta announced it in March 2021. In addition, "***these projects will also facilitate China's efforts to expand scientific and technological cooperation, impose its tech standards internationally, further its technology transfer goals, and potentially enable politically motivated censorship.***"[13] To curb Chinese expansion, from 2021, India, the US, Japan, and Australia have agreed to invest $50 billion in digital infrastructure development in the Indo-Pacific region under the Quad Initiative as the Internet-enabling cable launched from Singapore, connecting peninsular Southeast Asia to US mainland, and Indonesia will be beneficiary of what is the world's longest fibre-optic telecom cable.[14] G7 in 2021 also agreed to launch Partnership for Global Infrastructure and Investment as a Western alternative for developing countries to Chinese infrastructure investment. India's burgeoning SCs network is also noted. In February 2022, Bharti Airtel, India's leading telecom provider, joined the SMW6 (Southeast Asia – Middle East-West Europe 6) SC to upgrade the high-speed network for India's emerging digital economy.[15]

Therefore, submarine infrastructure management deserves a strategic rethink and new market regulation. This is especially true for Europe, which is seeking its own technological and digital sovereignty in the Mediterranean Sea. The Italian BlueMed SC, recently activated by Telecom Italia Sparkle S.p.A., and the SCs for ultrafast digital connections envisioned by the India-Middle East-Europe Economic Corridor (IMEC), approved at the 2023 G20 New Delhi Summit, should be seen in this light.[16] The Mediterranean is a rather congested space in terms of the number of vital cables running through it, confirming its centrality in the field of SCs as well.

[13] US Department of Defense. "Assessment on U.S. Defense Implications of China's Expanding Global Access." (2018), available at ***https://media.defense.gov/2019/Jan/14/2002079292/-1/-1/1/EXPANDING-GLOBAL-ACCESS-REPORT-FINAL.PDF***; see also Wen, Yun. "Huawei's Expansion into the Global South: A Path Toward Alternative Globalization?" ***Huawei Goes Global: Volume I: Made in China for the World*** (2020): 147-169; and Ehl, David. "Africa Embraces Huawei Technology Despite Security Concerns," ***Deutsche Welle*** (2022), ***https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700***

[14] Mcbeth, John. "US, Indonesia in digital challenge to China's BRI." ***Asia Times*** (2020).

[15] PTI. "Bharti Airtel joins SEA-ME-WE-6 undersea cable consortium; anchoring 20 pc investment in cable system." ***The Economic Times|Industry*** (2022).

[16] Chirafisi, Paolo, and Pezzulli, Bepi. "La geopolitica dei cavi sottomarini: da Nuova Dehli a Genova, prende forma l'Indo-Mediterraneo." ***ProiezionidiBorsa*** (2023).

2. Submarine Cables: a primer

There are two main types of SCs: submarine communications cables, used to transmit data, and submarine power cables, used to transmit electricity, from one place to another, both are designed for underwater use and typically laid/buried in the seabed.[17] The first type is the basis of this paper.

International submarine fibre-optic cable networks are a true "***bridge between people***," unique in their technical nature, their vital importance to the economy and security, and their vulnerability. SCs have been used for long-distance communications since the laying of the world's first cable at Dover Strait in 1850.[18] 165 years after UK Queen Victoria sent the inaugural message to US President James Buchanan on the cable, copper has given way to fibre optics and gutta-percha to polyethene, and SCs started to "***outperform satellites in terms of volume (only 3%), speed and economy of data and voice communications***"[19] remaining the most efficient way to send information.[20] Admiral James Stavridis, US Navy (Ret), former NATO Supreme Allied Commander, wrote, "***It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy. We have allowed this vital infrastructure to grow increasingly vulnerable and this should worry us all,***"[21] and suggested, "***In the case of heightened tensions, access to the underwater cable system represents a rich trove of intelligence, a potential major disruption to an enemy's economy and a symbolic chest thump.***"[22]

Cables can interconnect with each other, with terrestrial networks, and with other social and technological infrastructures, forming the backbone of the global Internet. It means that damage to a cable in one location could affect service to other cables serving other locations. Despite their status as critical infrastructure, SCs remain vulnerable to a range of attacks and cybersecurity challenges - no wonder they are mentioned in the NIS2 Directive. Since September 11th, concern has grown about SCs as targets, particularly intentional interference by state and non-state actors that includes damage to SCs on the seafloor, and cable landing stations, as well as cyberattacks when perpetrators break into the network management systems used to operate cable systems.[23] The revelation by Snowden that the US and UK have engaged in the "***largest suspicionless surveillance program in human history, tapping directly into the backbone of Internet***,"[24] i.e., fibre-optic cables, has catapulted the issue to the forefront

[17] Intagliata, Christopher, and Sweeney, Marlisse S. "What links the global Internet? Wires inside tubes no bigger than a garden hose." ***The World*** (2015); see also Woollaston, Victoria. "Messages From the Deep: Interactive Map Plots the Sprawling Growth of the Submarine Cable Network Since 1989." ***Daily Mail*** (2014).
[18] Fouchard, Gérard. "Historical overview of submarine communication systems." ***Undersea Fiber Communication Systems***. Academic Press, 2016. 21-52.
[19] Schwartz, Mischa, and Hayes, Jeremiah. "A history of transatlantic cables." ***IEEE Communications Magazine*** 46.9 (2008): 42-48.
[20] APEC Policy Support Unit. "Economic Impact of Submarine Cable Disruptions." (2012), available at ***http://bitly.ws/yzJ2***
[21] Sunak, Rishi. ***Undersea cables: indispensable, insecure***. Policy Exchange, 2017.
[22] Stavridis, Jim. "A new cold war deep under the sea?" ***The Huffington Post*** (2016).
[23] Id. at 1; see also Sanger, David E., and Schmitt, Eric. "Russian ships near data cables are too close for US comfort." ***The New York Times*** (2015).
[24] MacAskill, Ewen, et al. "GCHQ Taps Fibre-optic Cables For Secret Access to World's Communications." The Guardian (2013); see also Street, Jon. "Wikimedia among nine groups suing the NSA for tapping directly into the Internet backbone." The Blaze (2015).

of global discourse. However, seabed warfare began as early as the Cold War, with the US Navy's Operation Ivy Bells to intercept the communication links of Soviet submarines.[25] Russia, on the other hand, had a specific directorate for deep-sea operations, known as GUGI, capable of laying sensors, interdicting others' infrastructure and surveying the seabed. In addition, China had the ability to extract signals from cable fibres using surface technology. Since then, the size of seabed infrastructure networks and the dependence of civil society on these networks have exploded. Thus, there is a "***real and present threat***."[26]

According to the consulting firm Market Research, the huge submarine fibre-optic cable market will rise from $18.2 billion in 2022 to $48 billion in 2030, with a growth rate of 12.9% over the 2022-2030 period.[27] Also, in the same period, global mobile data traffic is expected to increase at a compound annual growth rate of nearly 28%, reaching 603.5 million Tb/month. [28] Thus, the business imperatives of Big Tech companies and the need to meet the demand for bandwidth, aimed to expand coverage to serve new regions and customers, and to generate new revenue emerge as the main drivers for developing SCs.

2.1 Development and Industry

A submarine telecom cable has been defined as "***a cable laid in the seabed, or buried in shallow water, intended to carry communications.***"[29] As thick as a garden hose, these cables consist of fibre-optics in the core coated with different materials to last up to 25 years (Figure 2). This physical wrapping protects the optical fibres from signal degradation as well as damage. In recent years, the capacity of SCs has increased from hundreds of Mb/s to hundreds of Tb/s.[30] In 2021, Google's Dunant SC connecting the US to Europe set a record for capacity and data rate using space-division multiplexing technology, also called high fibre count, and other innovations are being considered, such as multi-core fibre cables that add two or more optical cores, doubling the capacity of the fibre. If the growth in demand for bandwidth from SCs continues unabated, the industry may have no choice in the future but to commercialize Pb/s cables (where 1Pb/s is 1,000,000,000,000,000 bit/s – astounding!) or build many more SCs of lower capacity.

[25] Mauri, Paolo. "Sottomarini, sabotaggi e risorse: l'ombra dell'Underwater Warfare negli oceani." ***Il Giornale*** (2023).
[26] Salerno-Garthwaite, Andrew. "Seabed warfare is a real and present threat." ***Naval Technology*** (2022).
[27] Market Research. "Submarine Optical Fiber Cables." ***Global Industry Analysts*** (2023).
[28] "Submarine cable systems Global Market Report 2023." ***The Business Research Company***, 2024.
[29] ITU. "Submarine Cable Regulation", ***PowerPoint presentation*** (2010), available at ***https://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/Dakar-10/PDF/cable_sous_marin.pdf***
[30] Thomas, Robert, et al. "Technology in Undersea Cable Systems: 50 Years of Progress." ***Marine Technology Society Journal*** 49.6 (2015): 88-109.

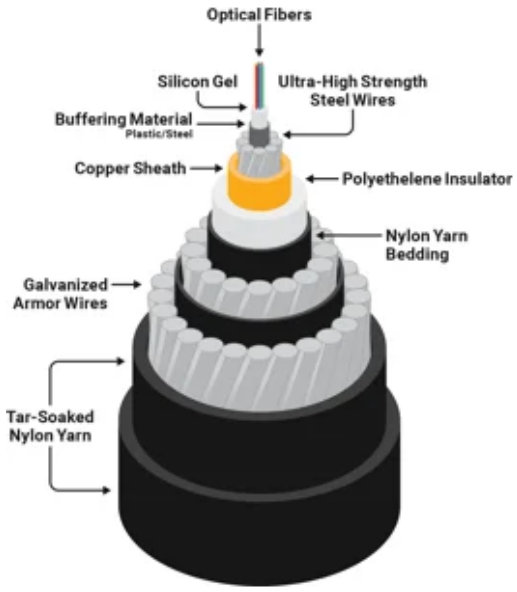

Figure. 2 – Diagram of a SC (Source: TeleGeography).

As in Figure 3, a SC system is divided into two parts: the "***wet***" system, which consists of the cable itself and repeaters or amplifiers placed along the cable to boost the signal, over regular intervals (≅100km), and the "***dry***" system, in which the cable comes ashore, is run through a manhole on the beach, to be connected to terrestrial networks and routed to its final location. The landing station typically contains equipment to control the transmission and reception of data flow, power, and network management.[31] Fencing and barbed wire at cable landing stations are among the measures for the physical protection of the cable. Cables are laid on the seabed by specially designed vessels known as cable layers (e.g., US Navy's Zeus). In general, the SC-laying process takes 1 to 3 years to bring the system from route planning to an operational resource. In deep water, cables are laid directly on the seabed. In contrast, when approaching the coast, specialized plows are used to bury them in trenches for protection and insulation, as well as lining them with galvanized steel armour.[32]

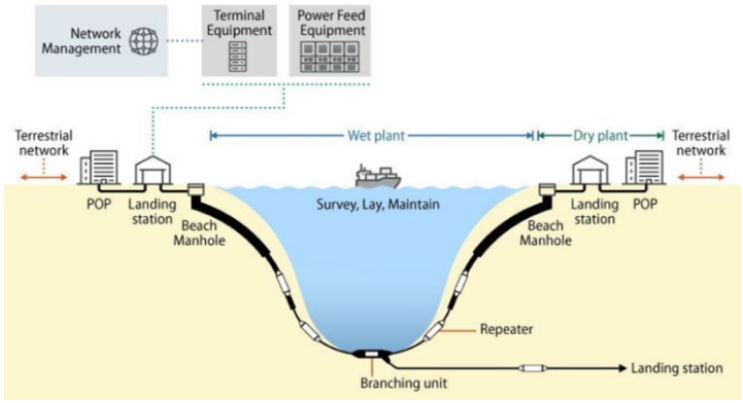

Figure. 3 – Submarine telecom cable system (Source: CRS).

[31] Swinhoe, Dan. "What Is a Submarine Cable? Subsea Fiber Explained." ***DatacenterDynamics*** (2021).
[32] Gallagher, Jill C. "Undersea Telecommunication Cables: Technology Overview and Issues for Congress." ***Congressional Research Service R47237*** (2022).

In addition, SCs can prove invaluable for scientific development. Intelligent SCs are being developed (e.g., the SMART - Science Monitoring and Reliable Telecom initiative) that integrate sensors in and around repeaters, thereby supporting the blue economy through oceanographic data collection, helping to improve the resilience of individual cable systems and the entire communication network, and accelerating climate change and disaster risk warning strategies.[33]

Years ago, SCs were initially owned by telecom companies that would band together to form a consortium of all the parties interested in using the cable. As time went on and the Internet grew in the late 1990s, more companies saw the potential of investing in the infrastructure. In fact, the capacity added to the overall SCs network by private companies far outpaced the growth of traditional telecom ones. Major companies specialized in construction, laying, maintenance, and repair/replacement of SCs include American SubCom, French Alcatel Submarine Networks (ASN), Italian Prysmian Group, British Global Marine in the North Atlantic area, Japanese NEC Corporation, and Chinese HMN Tech Co. Ltd. Cable owners and investors contract repair services to these companies, which have the ships, personnel, and resources to carry out repairs in the middle of the ocean quickly. The total number of cable repair vessels in service, whether installing a new cable or repairing a cable, is surprisingly low: about 60.

Among the three main ownership models, the most common is the consortium or multiple-owner system.[34] This model sees a group of commercial entities (e.g., companies participating in agreements with others, such as public-private partnerships like Telecom Namibia-Paratus Telecom)[35] interested in capacity along a given route pooling their resources to build the cable, then sharing the capacity and the resulting benefits, but also the risks. About 90% of funding for SCs over the past three decades has come from consortia, totalling $43 billion.[36] Multilateral development banks, such as the World Bank, also finance some submarine projects. These development banks offer lower interest rates, more flexible terms, and are more forgiving of default than commercial debt alternatives.[37] Most of the $3.2 billion financed by development banks has gone to link African nations. A single-owner system (e.g., nation-state backed entities,[38] private companies including hyper scalers like Google, Meta, Microsoft, and Amazon) can finance the expense of a cable, either for its own use or to resell capacity to others. Yet this sector is undergoing a major shift, with Big Tech reshaping the SCs ecosystem.[39] This has implications for both the global security architecture and the broader geography of the Internet, which is mostly located in highly industrialized countries (i.e., techno-spheres) and monopolized by a handful of companies, which through a network of submarine fibre-optic cables control Internet access, reversing a paradigm that originated with the invention of the telegraph, and weave a network of fibre-optic power (see Section 3.2).

[33] Howe, Bruce M., et al. "SMART subsea cables for observing the earth and ocean, mitigating environmental hazards, and supporting the blue economy." ***Frontiers in Earth Science*** 9 (2022): 775544.

[34] Gordon, Lori W., and Jones, Karen L. "Global communications infrastructure: undersea and beyond" ***The Aerospsace Corporation*** (2022), available at https://csps.aerospace.org/sites/default/files/2022-02/Gordon-Jones_UnderseaCables_20220201.pdf

[35] Myles. "Telecom Namibia and Paratus announce major public private partnership to connect Namibia to Google's New Undersea Cable." ***Extensia*** (2021).

[36] Id. at 6.

[37] Frascà, Domenico, and Galantini, Luca. "The Issue of Submarine Cable Security." ***Towards a New European Security Architecture*** (2023): 51.

[38] Some governments have invested in cables. For example, Tonga-Fiji Submarine Cable System is owned and operated by TCL, which developed and manages the cable with financing support from the Asian Development Bank and World Bank. TCL is a public enterprise 80% owned by the government. In China, three SOEs - China Mobile, China Telecom, and China Unicom - invested in undersea cables. In the United States, the U.S. Navy owns over 40,000 nautical miles of various subsea cables.

[39] Gervasi, Phil. "Diving Deep into Submarine Cables: The Undersea Lifelines of Internet Connectivity". ***Kentik*** (2023).

More than one hundred SC breaks occur each year and "***Even after 100+ years of technological advancement, the process to repair subsea cables remains difficult [...] These are costly repairs for companies that have a direct impact on communication between continents.***"[40] Repair times vary depending on the severity of the damage. In some cases, cable damage may have a severe impact on digital connectivity causing long and extensive service interruptions, especially if there are no redundancy and contingency plans. In some cases, the cable industry and many countries have rerouting arrangements to ensure digital flows when failures occur on terrestrial lines or satellite networks.[41] In other cases, the damage can be repaired quickly, the impact is minimal and goes largely unnoticed by end users. At the regional level, the Atlantic Cable Maintenance and Repair Agreement and Mediterranean Cable Maintenance Agreement offer a dedicated fleet to maintain members' cables.

Governments worldwide currently grant licenses to strengthen geopolitical alliances, favouring companies based in friendly countries for diplomatic reasons. In the EU, three companies are particularly active in the Internet infrastructure sector in the Mediterranean region: Telecom Italia Sparkle, Orange, and Telxius, which are based in Italy, France, and Spain, respectively, all countries that are key gateways for telecom. Member states' diplomatic relations with countries in the region often help these companies secure contracts. For example, positive relations between France and Sahel countries have helped Orange obtain licenses in that region. Italian diplomatic efforts to maintain positive ties with Libya and Israel have helped Sparkle launch infrastructure projects in those countries (see Section 4). There is a similar relationship with multinational consortia that states authorize to operate SCs. For example, the Africa-1 cable, connecting Europe to Pakistan and East Africa, is operated by a consortium of companies based in Saudi Arabia, Egypt, and the United Arab Emirates as part of their cooperation to limit Iranian influence in their neighbourhood.

2.2 The Most Likely Threats

SCs, the information highways that underpin the global economy and facilitate telecom worldwide, operate in a dynamic risk environment contending with geopolitical, physical, cyber, and other threats.[42] Three major areas where SCs are vulnerable: physically at sea, physically when they emerge onto land, and digitally via their network management systems. Some scholars distinguish three kinds of danger to the functioning of the cable network: natural disasters, accidents that arise from multi-use conflicts, and deliberate attacks;[43] see (Figure 4). Out of these, the second type frequently occurs and the third is most troublesome.[44]

[40] Jayawardena, Raj. "Seeing Under the Sea in 2023" ***ISE Magazine*** (2023); see also Wagner, Eric. "30,000 Feet Below: Connecting Continents from the Ocean Floor." ***AT&T Technology Blog*** (2017).

[41] WG8. "Final Report Protection of Submarine Cables through Spatial Separation." ***CSRIC*** (2014), available at ***https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf***; see also Brandon, John. "Protecting the Submarine Cables That Wire Our World." ***Popular Mechanics*** (2013).

[42] Recorded Future. "The Escalating Global Risk Environment for Submarine Cables." ***Insikt Group*** (2023), available at ***https://www.recordedfuture.com/escalating-global-risk-environment-submarine-cables***

[43] Bueger, Christian, Liebetrau, Tobias, and Franken, Jonas. "Security threats to undersea communications cables and infrastructure–consequences for the EU." ***Report for SEDE Committee of the European Parliament, PE702*** 557 (2022).

[44] Carter, Lionel. ***Submarine cables and the oceans: connecting the world***. No. 31. UNEP/Earthprint, 2009.

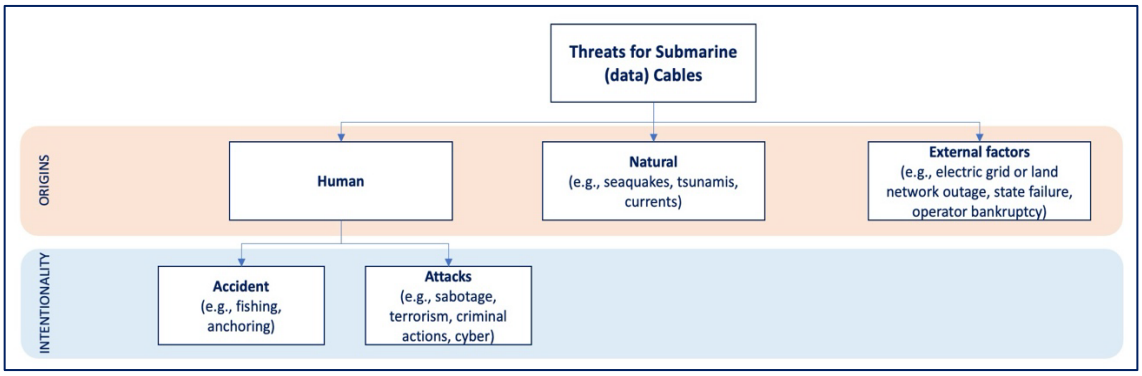

Figure. 4 – Recap of possible threats for SCs (Source: Authors' elaboration).

First are physical hazards: natural disasters or human accidents. Seaquakes, rocks or sharks could damage the cables, disrupting the data flow and requiring specialized contractors to restore them.[45] In 2022, volcanic eruption severed Tonga's connection to the world, which was restored after many weeks by SubCom's ship Reliance.[46] In June 2023, a natural ice shift disrupted SC serving Alaska's North Slope, compromising Internet and cellular service for residents of this Arctic area.[47] As the impact of climate change on the oceans will lead to more severe weather events, such threats to cables are likely to increase in the near future. At the same time, environmental threats caused by SCs are analysed,[48] and some studies found no or only minor impacts,[49] while others report substantial ones.[50] Near the coasts, moreover, human activities, particularly fishing, dredging or anchoring pose additional risks to their integrity.[51] Some propose the creation of protection zones that safeguard SCs and place appropriate restrictions on activities around them.[52] In 2017 a SC was accidentally severed by a ship off the coast of Somalia, causing three weeks Internet outage costing the country $10 million a day.[53] In November 2021, parts of SC located near Svalbard Islands mysteriously disappeared, compromising LoVe observatory.[54] In January 2022, the cable connecting SvalSat station to mainland and NASA broke, causing the loss of years of scientific data.[55]

Second are criminal threats, ranging from theft of sensitive information to gain a competitive advantage to terrorism, sabotage, or vandalism.[56] ASN said, "***Our main responsibility is to protect our customers' confidential information and maintain their privacy.***" Rivals might not only tap into cables for intelligence gathering, espionage and surveillance but also cut them to cause isolation of enemy

[45] Schaub Jr, Gary, Martin Murphy, and Frank G. Hoffman. "Hybrid maritime warfare: Building Baltic resilience." ***The RUSI Journal*** 162.1 (2017): 32-40; see also Sechrist, Michael. ***New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems***. Harvard Kennedy School, Belfer Center for Science and International Affairs, 2012.

[46] Associated Press. "Tonga's Internet Is Restored 5 Weeks After Big Volcanic Eruption," ***NPR.org*** (2022); see also Duckett, Chris. "Digicel Reconnects Tongan Users via Satellite to Rest of the World," ***ZDNet*** (2022); and Folau, Linny, and Fonua, Mary Lyn. "Torn Apart, Missing 110km Domestic Fibre Optic Cable May Take Year to Replace." ***Matangi Tonga Online*** (2022).

[47] Knight, Greg, and Klint, Chris. "Cut Cable Causes Internet and Cellphone Outages in Arctic Alaska," ***Alaska Public Media*** (2023); see also Naiden, Alena. "Internet and Cell Outages in Northwest Alaska, North Slope Caused by Offshore Fiber Optic Cut." ***Anchorage Daily News*** (2023).

[48] Harris, Peter T. "Anthropogenic threats to benthic habitats." ***Seafloor geomorphology as benthic habitat***. Elsevier, 2020. 35-61.

[49] Ragnarsson, Stefán Áki, et al. "The impact of anthropogenic activity on cold-water corals." ***Marine Animal Forests: The Ecology of Benthic Biodiversity Hotspots*** (2017): 989-1023; see also Clare, M. A., et al. "Climate change hotspots and implications for the global subsea telecommunications network." ***Earth-Science Reviews*** 237 (2023): 104296.

[50] Taormina, Bastien, et al. "A review of potential impacts of submarine power cables on the marine environment: Knowledge gaps, recommendations and future directions." ***Renewable and Sustainable Energy Reviews*** 96 (2018): 380-391.

[51] Carter, Lionel, et al. "Insights into submarine geohazards from breaks in subsea telecommunication cables." ***Oceanography*** 27.2 (2014): 58-67; see also Ardelean, Mircea, and Minnebo, Philip. "HVDC submarine power cables in the world." ***Joint Research Center*** (2015); and Davenport, Tara. "Submarine communications cables and law of the sea: Problems in law and practice." ***Ocean Development & International Law*** 43.3 (2012): 201-242.

[52] Matley, Holly Elizabeth. "Closing the gaps in the regulation of submarine cables: lessons from the Australian experience." Australian Journal of Maritime & Ocean Affairs 11.3 (2019): 165-184; see also Id. at 20.

[53] Associated Press. "Somalia back online after entire country cut off from internet for three weeks." ***The Guardian*** (2017).

[54] Kirk, Lisbeth. "Mysterious Atlantic Cable Cuts Linked to Russian Fishing Vessels." ***EUobserver*** (2022).

[55] "The Svalbard Fibre Optic Cable Connection." ***Space Norway*** (2022).

[56] Chalfant, Morgan, and Beavers, Olivia. "Spotlight Falls on Russian Threat to Undersea Cables." ***The Hill*** (2018); see also "Concern over Russian Ships Lurking Around Vital Undersea Cables." ***CBS News*** (2018); and Sanger, David E., and Schmitt, Eric. "Russian Ships Near Data Cables Are Too Close for U.S. Comfort." ***New York Times*** (2015).

communications, with serious consequences for its economy.[57] In wartime, "***cables and nodes would be prime targets of a hybrid warfare campaign***" and threatened by grey zone operations.[58] Attacks can also come from hacktivists and ransomware groups, who aim to disrupt infrastructure as a show of force. Saverio Lesti argues that "***seabed warfare is the key element of a state's strategic position during a conflict,***" and if governments aim to mitigate these threats "***diversify routes to reduce the risk of a single attack, improve security with surveillance systems, and develop international agreements.***" Others note that "***landing stations are the most accessible and impact-rich targets as they are concentrated in a handful of coastal locations.***"[59] In 2022, there were two incidents of SC cutting in France[60] and a double cut of the land segment of SEA-ME-WE-5 (Southeast Asia-Middle East-Western Europe-5) SC in Egypt, both of which compromised communications in different parts.[61] In September 2022, Nord Stream pipeline sabotage led to the awareness - belatedly - of the fragility of SCs and was followed by damage to nearby Shefa-2 cable.[62] In the wake of this attack, the UK Ministry of Defense has increased the protection of SCs and conducted a threat assessment of cables landing in Ireland, a major hub for cables connecting the US, UK, and Western Europe.[63] In addition, the British Royal Navy has prioritized the procurement of two Multi-Role Ocean Surveillance ships by 2023. Proposed responses are militarily increased naval patrols, surveillance activities, national focal points, and mapping on navigational charts.[64] Yet, this also implies that it is public knowledge where the cables are laid, meaning they are put at risk of deliberate attacks.

Also, geography and the degree to which countries are dependent on infrastructure can shape exposure to risks. Cable failures could have a more severe impact on islands and chokepoints. Ibiza, for instance, depends on one connection, Sardinia depends on three cables and Malta on five. Sicily represents "***the centre of Italy's connectivity,***" as its coasts are traversed by regional and global networks. Our country is an integral part of the global networks system, which is why Eurispes speaks of the "***triple threat***" to Italy, highlighting that SCs in our seas are exposed to the risk of "***fortuitous damage due to some fishing techniques, sabotage carried out ashore at cable docking points, and cyberattacks on the IT infrastructures of the countries involved in the hybrid conflict with Moscow.***"[65] In general, the SCs that cross the Italian seas all have local, regional, and global significance: some start in Italy, others terminate there and still others pass through.

Some scholars observed, "***connecting cable sites with software creates more efficiency and provides operators greater operational awareness...it creates potential new risk, particularly to***

[57] Khazan, Olga. "The Creepy, Long-Standing Practice of Undersea Cable Tapping". ***The Atlantic*** (2013).
[58] Id at 44.
[59] AEP. "Threats to Undersea Cable Communications." ***US Dep. of Homeland Security. Office of Intelligence and Analysis*** (2017), available at ***https://www.hsdl.org/c/abstract/?docid=870379***
[60] Brent, Thomas. "Mass Attack on Internet Cables in France Almost Professional." ***The Connexion*** (2022).
[61] PTA. "Dual cut in the terrestrial segment of SEAMEWE-5." (2022); see also Sharwood, Simon. "Submarine Cable Damage Brings Internet Pain to Asia, Africa." ***The Register*** (2022); and Moss, Sebastian. "AAE-1 Cable Cut Cause Widespread Outages in Europe, East Africa, Middle East, and South Asia." ***DCD*** (2022); and Madory, Doug. "Outage in Egypt Impacted AWS, GCP, and Azure Interregional Connectivity." ***Kentik*** (2022).
[62] Woody, Christopher. "Suspected Nord Stream Sabotage Shows 'Vulnerability' of Everything We Build on the Seabed, Top British Admiral Says." ***Insider*** (2022).
[63] Mooney, John. "Defence Forces Assess Risk to Subsea Cables amid Fears of Russian Attack." ***The Times*** (2022).
[64] Matis, Michael. "The protection of undersea cables: A global security threat." ***US Army War College***, 2012; see also Martinage, Robert. "Under the sea: The vulnerability of the commons." ***Foreign Aff.*** 94 (2015): 117; and Id. at 20.
[65] Eurispes. "35° Rapporto Italia". (2023), available at ***https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/05/24142258/sintesi-rapporto-italia-2023.pdf***

cyberattacks."[66] Malicious actors, from foreign spies to criminal gangs, may leverage information technologies to harm SC operations. They could attempt to spy on or even manipulate, degrade, or disrupt Internet traffic flows altogether. Among others, according to Reichmann, Russia threatens enemy SCs.[67]

The relentless push for expanded bandwidth capacity has led cable system operators to embrace advanced web-based ICT, potentially enabling cyberattacks that exploit third-party vulnerabilities. Increasingly, companies are using "***remote network management systems***" to remotely control the functionality of SCs.[68] Nevertheless, while this strategy saves costs, it increases exposure to cyber risks, often through poorly protected software.[69] Installing viruses, such as backdoors in cable landing stations, can be one tool of cyber espionage, but not the only one.[70] Coordination of security efforts is complicated by the coexisting presence of companies and governments in the SC infrastructure. The convergence of financial interests may result in potential divergence in objectives and priorities, making it challenging to enforce a coherent security approach. This raises questions about data protection within this context, susceptible to improper exploitation. Deterrence measures can play a role. In April 2022, the US Dep. of Homeland Security revealed to have foiled a cyberattack on a SC that carried Internet traffic and other data to Hawaii and the surrounding region. This attack was enabled by a credentials-related breach of a third party.[71]

Threats from cyber-attacks and espionage (e.g., wiretapping) are different from physical attacks and may be exacerbated by recent geopolitical developments.[72] In most cases, these attacks seek to access the data carried by the cable and may not cause physical damage to the cable itself. Cables are likely to be targets of criminal attacks due to escalating tensions between states (e.g., in February 2023 two SCs connecting Taiwan-controlled Matsu islands were cut, probably deliberately tampered with by Chinese a fishing vessel).[73] Organizations and governments should work diligently to prevent this lifeblood from being compromised, encrypt their communications, and adopt best cybersecurity practices to mitigate risk. Europe encourages information sharing and community governance of cable networks. Cybersecurity is not just about data, but also about the means through which data is transmitted, and thus the protection of Submarine Line Termination Equipment (SLTE) and all associated systems for the correct functioning of cables (e.g., electric energy).

2.3 A Touch of Regulation

[66] Id. at 44 and 63; see also Ross, Margaret. "Understanding interconnectivity of the global undersea cable communications infrastructure and its implications for international cyber security." ***The SAIS Review of International Affairs*** 34.1 (2014): 141-155.

[67] Reichmann, Deb. "Could Enemies Target Undersea Cables That Link the World?" ***AP News*** (2018).

[68] Sherman, Justin. "Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security." ***Atlantic Council*** (2021), available at ***https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf*** (The report states that hackers could "breach multiple remote network management systems used to control different submarine cables to completely disrupt the flow of Internet data across that infrastructure." It also notes that hacking a submarine cable may be easier than physically tapping cables, as it can be done remotely.); see also Sherman, Justin. "The U.S. Should Get Serious About Submarine Cable Security." ***Council on Foreign Relations*** (2021).

[69] Sherman, Justin. "Cybersecurity under the Ocean: Submarine Cables and US National Security." ***Aegis Series Paper No. 2301*** (2023), available at ***https://www.lawfareblog.com/cybersecurity-under-ocean-submarine-cables-and-us-national-security***

[70] Voelsen, Daniel. "Cracks in the internet's foundation: The future of the internet's infrastructure and global internet governance." (2019): 35.

[71] Temple-Raston, Dina, and Powers, Sean."Who tried to hack Hawaii's undersea cable?" ***The Record From Recorded Future News*** (2022).

[72] Id. at 41.

[73] Wu, Sarah, and Lee, Yimou. "Fear of the dark: Taiwan sees wartime frailty in communication links with world." ***Reuters*** (2023).

NATO CCDCOE recognizes the strategic importance of SCs and the dependence of states on their operation.[74] However, safeguarding this critical infrastructure in both peacetime and war faces significant challenges. A SC navigates different environments: land or sea, on the one hand, and cyber or physical space, on the other. This heterogeneity of environments results in a dispersed regulatory framework.[75] Moreover, they mostly rest on the bottom of international waters. Very often ownership is divided among multiple companies and Institutions from different states and jurisdictions. This again underscores a feature of the digital environment: the convergence of public and private elements, which increasingly intersect with each other. The provisions governing SCs date back to the 1884 International Convention for the Protection of Submarine Telegraph Cables, now part of the 1982 United Nations Convention on the Law of the Sea (UNCLOS), which replaced the 1958 Geneva Convention on the High Seas. Accordingly, "***submarine communication cable***" refers to any cable owned, operated, or laid by a state, and privately-owned cables licensed by the state for telecom traffic. The Tallinn Manual addresses the issue of SCs, stating in Rule 54 that states enjoy sovereignty over SCs in their territorial sea and "***they are treated in the same fashion as cyber infrastructure located on land territory.***" The North Atlantic Command, among others, is tasked with monitoring and protecting against threats to submarine infrastructure.[76] Because most of this undersea infrastructure is owned by private companies, it is complicated to prove an attack on a state and identify the governments that sponsor the attacks. Given that the undersea environment simultaneously offers resources (data, energy, mining) and is an arena of active infrastructure conflict, international encounters, and competition between different ambitions, which, as noted above, can also express itself through crimes, one might also think of defining a new domain, that of "***undersea warfare.***"

In conclusion, in a context of rising tensions and non-war conflicts, the watchword is protection, which must go hand in hand with technological innovation and cooperation among allied countries. Three types of approaches can be adopted: the regulatory approach, which ensures shared rules for the laying, maintenance and surveillance of SCs; the military approach, which employs ships and submarines for the proper functioning of submarine infrastructure and guards in the event of a threat; and the redundancy approach, whereby each country is connected to the outside world through multiple SCs, to limit the negative economic and strategic impact in the event of a cable malfunction, avoiding a total communications blockade that would pose an existential threat to the security of states.

[74] NATO CCDCOE. "Strategic importance of, and dependence on, undersea cables." ***NATO Cooperative Cyber Defense Centre of Excellence*** (2019), available at ***https://ccdcoe.org/library/publications/strategic-importance-of-and-dependence-on-undersea-cables/***

[75] Morel, Camille. ***L'Etat et le réseau mondial de câbles sous-marins de communication***. Diss. Lyon, 2020.

[76] PA Media. "UK military chief warns of Russian threat to vital undersea cables." ***The Guardian*** (2022).

3. The Infrastructure of the Digital Age: power competition and economic implications

The issue of digital SCs poses significant challenges for geopolitics. Indeed, it will also be a geopolitical game, in which each country will want to assert its leadership and standards, turning into a new arena of competition between Powers to reassert their international hegemony in changing the global order. Some scholars have interpreted the rise of the US in the 20th century by considering the country's efforts to take control of SCs.[77] Cables establish forms of transnational relations that often extend or transcend conventional bilateral or regional forms of cooperation.

Some countries have an important geographic position in the international cable system, acting as connecting points between political regions. Contemporary geopolitical dynamics manifest themselves in two main aspects: geopolitical competition between states and the rise of transnational technology companies as geopolitical actors. Certainly, geopolitical competition revolves primarily around two centres of gravity – the US and China - but the promises of digital sovereignty,[78] technological sovereignty,[79] and data sovereignty[80] to reap economic benefits are increasingly evident worldwide. Among others, an example of the geopolitical importance of the SCs and its intertwining with digital sovereignty is the US Clean Network Program, announced in August 2020, which includes five lines of effort to counter China's influence on US telecom networks, mobile app stores, software apps, cloud computing, and SCs to safeguard sensitive information of citizens and companies from intrusion by malicious actors.[81] In March 2021, the EU Council adopted the "Data Gateways" declaration, which includes a series of calls to action for new SC infrastructure in the European neighbourhood (Western Balkan, the Arctic region, Africa, Latin America, Southeast Asia). These connections provide alternative routes for global Internet traffic and support Internet security, stability, and resilience. Strengthening connectivity around the EU can be seen as four platforms, each of which has specific geopolitical significance: the Atlantic, the Mediterranean, the North Sea and the Arctic, and the Baltic to Black Sea corridor. EU Global Gateway launched in December 2021 to fund international projects (e.g., expansion of the BELLA program, with EllaLink SC connecting Europe (through Sines, Portugal) to Latin America

[77] Hills, Jill. ***The struggle for control of global communication: The formative century***. University of Illinois Press, 2010; see also Winkler, Jonathan Reed. ***Nexus: strategic communications and American security in World War I***. Harvard University Press, 2008; and Smith, Jason W. ***To Master the Boundless Sea: The US Navy, the Marine Environment, and the Cartography of Empire***. UNC Press Books, 2018.

[78] Pohle, Julia, and Thiel, Thorsten. "Digital sovereignty." ***Pohle, J. & Thiel*** (2020); see also Ganz, Abra, Camellini, Martina, Hine, Emmie, Novelli, Claudio, Roberts, Huw and Floridi, Luciano. "Submarine Cables and the Risks to Digital Sovereignty" (2024), available at SSRN ***https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4693206#***

[79] Floridi, Luciano. "The fight for digital sovereignty: What it is, and why it matters, especially for the EU." ***Philosophy & technology*** 33 (2020): 369-378; see also Hong, Yu, and Goodnight, G. Thomas. "How to think about cyber sovereignty: The case of China." ***China's Globalizing Internet***. Routledge, 2022. 7-25; and Mueller, Milton L. "Against sovereignty in cyberspace." ***International studies review*** 22.4 (2020): 779-801.

[80] Hummel, Patrik, et al. "Data sovereignty: A review." ***Big Data & Society*** 8.1 (2021): 2053951720982012.

[81] U.S. Department of State. "The Clean network". (2020), available at https://2017-2021.state.gov/the-clean-network/index.html

(through Fortaleza, Brazil) and currently having the lowest latency on the market) competing with China's BRI and contributing to European digital autonomy.

Most EU funding is for Africa, like Medusa cable, jointly funded with AFR-IX Telecom, Orange, which will interconnect Southern European countries with EU's Southern neighbours by 2025, and EurAfrica Gateway cable, which will run from the Iberian Peninsula along the Atlantic coast of West Africa across the Gulf of Guinea to the Democratic Republic of Congo, also seeking to narrow the connectivity gap between coastal and inland States (cf. Africa Europe Digital Innovation Bridge) and to promote the digital sovereignty of the two continents by improving data flow and security standards. The intent is to connect underserved countries and build ties with strategic partners in the region like Nigeria, Africa's most populous country.

Another EU proposal is Far North Fiber, a SC that will connect Scandinavia to Japan through the Arctic to avoid major choke points such as the Suez Canal and the South China Sea. However, it is not only Western countries that are concerned with the crucial geopolitical role of SCs. While discussions among the BRICS countries (Brazil, Russia, India, China, and South Africa) about a shared SC system seem to have been abandoned, major international players, including individual BRICS countries, have or are planning to build their own SC networks to circumvent what they perceive as the US-dominated Internet and the associated surveillance risks demonstrated by the Snowden revelations.[82]

Whether small island states are dependent on one or two cables, whether they are in remote locations or in the process of development or economic recovery, or whether they are fragile and post-conflict states, efforts to secure SC connections should be included in development, peacebuilding, and capacity-building projects. The importance of cable infrastructure for democratic transitions, civil society participation and sustainable development should not be underestimated.

Until recently, highly specialized international players laid and managed the majority of SCs, but over the past decade it is increasingly Big Tech or state-owned companies that control this critical infrastructure,[83] now owning or leasing more than half of the submarine bandwidth and responsible for about four-fifths of planned cable investments. China's Huawei has invested heavily in SCs worldwide, with its subsidiary Huawei Marine, carrying out more than 90 projects from the Pacific to the Atlantic totalling more than 50.000 kilometres of SCs, before selling it in 2019 - a decision presumably linked to blacklisting by President Trump.[84] These trends also raise concerns about surveillance practices,[85] algorithmic governance,[86] and cybersecurity[87] that are shaped by Big Tech.

The question arises whether the SC network can be governed as a global common. Thus, the geopolitical dimension gets intertwined with commercial interests, as deploying Internet cables for thousands of

[82] Winseck, Dwayne. "The geopolitical economy of the global internet infrastructure." ***Journal of Information Policy*** 7 (2017): 228-267.
[83] Satariano, Adam, et al. "How the internet travels across oceans." ***The New York Times*** 10 (2019).
[84] Hasler, Jack. "Huawei Marine is being sold. That's unlikely to change the threat it poses." ***Washington Post*** (2019).
[85] Bauman, Zygmunt, et al. "After Snowden: Rethinking the impact of surveillance." ***International political sociology*** 8.2 (2014): 121-144; see also Gros, Valentin, Marieke De Goede, and Beste İşleyen. "The Snowden files made public: A material politics of contesting surveillance." ***International Political Sociology*** 11.1 (2017): 73-89; and Lyon, David. "Surveillance, Snowden, and big data: Capacities, consequences, critique." ***Big data & society*** 1.2 (2014): 2053951714541861.
[86] Amoore, Louise. ***Cloud ethics: Algorithms and the attributes of ourselves and others***. Duke University Press, 2020; see also Hansen, Hans Krause, and Porter, Tony. "What do big data do in global governance." ***Global Governance*** 23 (2017): 31.
[87] Christensen, Kristoffer Kjærgaard, and Liebetrau, Tobias. "A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry." ***Intelligence on the Frontier Between State and Civil Society***. Routledge, 2020. 85-98.

kilometres is expensive, and international Big Tech have increasingly entered the game with their own projects. The rise of Big Tech is linked to emerging and disruptive technologies, as well as the renewed rivalry between major powers. The entanglement is evident if one thinks of the SCs network as an economic trade route carrying the most important commodity of our information age: data.

3.1 Geography and network branching

Geography continues to be an integral element of international relations and a crucial feature of the digital environment.[88] Not surprisingly, geography shapes the configuration of the SC network and the positioning of SC hubs.[89] Following established naval routes, SCs as a public good serve as vehicles for data exchange, subject to geographical constraints.[90] For example, Portugal is positioning itself as data hub connecting Europe to Latin America. Nearly $48 billion has been invested in SC since 1990, and in recent days the Asia-Pacific region is affected by the laying of SCs.[91] Digital society is thus based on millennia-old trade lanes delineated by highly strategic and vulnerable gateways, known as chokepoints, which provide strategic routes between regions, the breakdown of which could lead to unpredictable economic and communication consequences. Among the chokepoints, the EU has properly recognized the growing importance of the Suez Canal, the geography of which features a concentration of several SCs that cross the Red Sea (recently damaged by sinking of cargo ships due to Houthi missile attacks)[92] from the Indian Ocean before reaching the Mediterranean Sea, mapping out a potential large-scale risk to the global Internet network in the face of an accident.[93]

Moreover, geography not only dictates the gateways but also the allocation of principal hubs for SCs. Before Brexit in 2020, transatlantic traffic flowed largely through the southwest coast of the UK to Europe, where the main cable hubs were Calais in France, Ostend in Belgium, and Zandvoort in the Netherlands. Since the Brexit vote, traffic has been diverted and diversified using new SCs bypassing the UK to other European countries, notably Ireland (e.g., HAVFRUE/AEC-2, WINS, IFSC cables).

Although small, the Mediterranean plays its part with historical continuity. Indeed, the ***Mare Nostrum*** is home to several significant hubs for Europe, operating as trade and information hubs with the Americas, Africa, the Middle East, and the Far East, via the Strait of Gibraltar, the Strait of Sicily, and the Suez Canal. These include the Marseille hub and the Sicily hub.[94] Marseille, which rose from 44th position in 2015 to 7th in 2022 among the world's Internet hubs, takes advantage of its central geographic location in the Mediterranean and is a crossroads for 16 SCs. Marseille also serves as the Internet Exchange Point (IXP) for the EU, along with Amsterdam, Frankfurt, Paris, and Sicily. Nodes in Catania, Mazara del Vallo, Palermo, and Trapani make Sicily a hub for Italy with a total of 19 transcontinental cables. Among other

[88] Kaplan, Robert D. "The revenge of geography." ***Foreign Policy*** 172 (2009): 96-105.
[89] Id. at 36.
[90] Starosielski, Nicole. ***The undersea network***. Duke University Press, 2015.
[91] Anastasio, Paolo. "Google progetta due nuovi cavi sottomarini dagli Usa al Giappone," ***Key4biz*** (April, 2024), ***https://www.key4biz.it/google-progetta-due-nuovi-cavi-sottomarini-dagli-usa-al-giappone/486651/***; see also Redazione Economia. "Google investe un miliardo di dollari per due nuovi cavi sottomarini dagli Stati Uniti al Giappone," ***Corriere della Sera*** (April, 2024), ***https://www.corriere.it/economia/innovazione/24_aprile_13/google-investe-un-miliardo-di-dollari-per-due-nuovi-cavi-sottomarini-dagli-stati-uniti-al-giappone-0a192aa4-37b4-4c59-a2fa-97466804fxlk.shtml***.
[92] Radio24. "Gli Houthi e l'attacco ai cavi sottomarini," (March, 2024), available at ***https://www.radio24.ilsole24ore.com/programmi/luogo-lontano/puntata/trasmissione-7-marzo-2024-160500-2397647948082567***; see also Redazione Adnkronos. "Mar Rosso, Rizzi (Ecfr): Danni ai cavi? No sabotaggio Houthi, ma superare colli bottiglia," (March, 2024), ***https://www.adnkronos.com/Archivio/internazionale/esteri/mar-rosso-rizzi-ecfr-danni-ai-cavi-no-sabotaggio-houthi-ma-superare-colli-bottiglia_5QrYMvbTUNJMeoQTPxAYyy***.
[93] Id. at 42.
[94] Id. at 36.

European trading points, Sicily is the closest hub to North Africa and the Middle East, a geographic feature that makes it the main Mediterranean gateway. In October 2023, a new IXP was born in Genoa thanks to an agreement between Sparkle and Ge-DIX (Genoa Data Internet eXchange).[95]

The Mediterranean offers efficient trade routes and reduced communications latency. Its geographic position, central among intercontinental lanes, makes it an important crossroads of connectivity - more submarine infrastructure is expected to be laid in the coming years. The links, built on choke points, place the Mediterranean at the centre and in a strategic position (e.g., new datacentre projects in North Africa) such that it attracts investment that fosters economic and technological development in the region and stability for security in the medium term. In addition, the Mediterranean, with the Indo-Pacific, is one of the most crowded competitive arenas because of the interconnections and overlaps of their political, economic, and military dimensions: hence Italy's commitment to best serve national interests in these two geopolitical regions.[96]

3.2 Sovereignty and control: Big Tech

Recent years have seen a sharp increase in SCs installations worldwide. Digitization and emerging/disruptive technologies are affecting the SCs industry. SC routes are proliferating and diversifying, mainly by private firms so-called Big Tech (or Tech Giants or Over-The-Top) who have become prominent investors in the industry, seeking to control data and networks for their own needs. While this phenomenon is welcomed for the improvement of global connectivity, it also shifts the balance of power by concentrating a key component of the global digital infrastructure in the hands of a few Big Tech, who are already providers of Internet services, content, cloud, and marketplaces. Until 2012, the share of global submarine fibre capacity used by Big Tech was less than 10%, but by 2022 it will be about 66%. SC are most likely to be owned by Alphabet, Meta, Amazon, Microsoft, or Alibaba. Apple has chosen to rely on specialized operators, while other Big Tech have managed, in less than 10 years, to take control of an industry previously dominated by traditional telecom companies. While telecom companies focus on their customers by providing communication links between city centres, Big Tech aim to maintain connectivity between their server farms that make-up their services, which means that their data centres on the ground determine where cables are laid.[97] Therefore, "***cloud***" is not only in the sky but also underwater and dependent on cable infrastructure. Both telecom companies and Big Tech have an economic interest in uninterrupted operations and in protecting cables from damage that will preserve their revenues. One notable project is Jupiter cable, from the US to Asia, built in partnership by Amazon, Facebook, NTT and SoftBank.[98] Big Tech both solely owns SCs (e.g., Google's Curie cable), participate in consortia (e.g., partnership between Google and Openserve for Equiano cable) or adopt other strategies (e.g., mergers and acquisitions to increase revenue expanding global presence).

Several Chinese companies, often directly affiliated with the Chinese Communist Party, invest in SCs. For example, Hengtong Group (and its subsidiary Huawei Marine) leads PEACE (Pakistan and East Africa

[95] "Nasce Ge-Dix, il Genova Data Internet Exchange." ***Liguria Business Journal*** (2023); see also A.S. "Sparkle, alleanza con Ge-Dix sul nuovo Internet Exchange Point di Genova." ***CorCom*** (2023).
[96] Osservatorio di politica internazionale. "Strategie di collegamento dell'Indo-Pacifico al Mediterraneo allargato. La prospettiva dell'Italia oltre il corridoio IMEC." ***Parlamento italiano N. 210*** (2023), available at ***https://www.parlamento.it/application/xmanager/projects/parlamento/file/repository/affariinternazionali/osservatorio/approfondimenti/PI0210.pdf***
[97] Burnett, Douglas R. "Submarine Cable Security and International Law." ***International Law Studies*** 97.1 (2021): 55.
[98] Id. at 36.

Connecting Europe) cable, which runs from Pakistan to France, extended from Pakistan to Singapore, and is a key piece of China's Digital Silk Road. For this reason, it has come under harsh warning from the US security apparatus, which has stated that it "***could be useful to the PRC government even if the cable is not commercially successful.***" Chinese SOEs - Huawei, Zte, China Telecom, China Mobile, China Unicom - have begun participating in large international consortia to build SCs such as WACS (West Africa Cable System), which connects South Africa to UK, and 2Africa Pearls,[99] which will become the longest SC, spanning over 45.000 kilometres, to connect Europe Asia Africa. The Chinese goal is to increase their political, economic, and technological influence in developing countries in Asia and Africa.[100]

Moreover, various SCs are set to land in India during the next few years.[101] Bharti Airtel participates in 2Africa Pearls and SMW6, Reliance Jio invests in IAX (India-Asia-Xpress) and IEX (India Europe Xpress), TEAS (Trans Europe Asia System) counts I-Squared Lightstorm as a supplier. These new routes connect different regions, making the network more redundant. With its long coastline, India appears to be a perfect location for additional cable landing stations connecting east and west. India also launched a SC between the Andaman and Nicobar Islands to the Indian mainland and inaugurated the Kochi-Lakshadweep Islands (KLI) SC from the mainland (Kochi) to 11 Lakshadweep Islands, funded by the Universal Services Obligation Fund. These cables will also enable the government to provide services through digital platforms, as well as create opportunities for people in the digital economy.

SMW6 SC demonstrated the growing geopolitical tensions over the SCs industry between the US and China, underscoring once again the geo-tech rivalry between the two countries. SMW6 will connect a dozen countries as it snakes its way from Singapore to France, crossing three seas and the Indian Ocean on the way. Without the intervention by the US government, Chinese HMN Tech would have won the supply contract for the SMW6 project against SubCom, NEC, and ASN. But Washington, fearful of Beijing's spies, ran a successful campaign to oust HMN Tech from the SMW6 project and have SubCom awarded the contract through pressure on consortium members.[102] Strategic importance of cables is borne out by the Trump Administration's intervention in 2019 to block the Pacific Light Cable Network (PLCN) designed by Facebook and Google to connect the US and Hong Kong, but approved with connections to the Philippines and Taiwan without Hong Kong for fear of espionage.[103] In 2018 Australia blocked the Chinese Huawei Marine connection between Sydney and the Solomon Islands.

Main driver for investment in SCs appears to be the growth of the data economy, which shows no signs of stopping in the near future and from which business opportunities, competition, and cooperation between industries and states can arise.[104] So far, Big Tech are not reselling capacity on cables that they

[99] Kim, Jonathan. "2Africa Subsea Cable Expands via PEARLS to 28k Miles, 33 Countries." ***Dgtl Infra*** (2021).
[100] Stein, Peter, and Uddhammar, Emil. "China in Africa: The Role of Trade, Investments, and Loans Amidst Shifting Geopolitical Ambitions." (2021), available at ***https://www.orfonline.org/public/uploads/posts/pdf/20230814142301.pdf***
[101] Kaur, Gagandeep. "The lowdown on India's burgeoning submarine cable network." ***Light Reading*** (2023).
[102] Brock, Joe. "U.S. and China wage war beneath the waves – over internet cables." ***Reuters*** (2023).
[103] Ibidem.
[104] Id. at 6.

have financed themselves; this investment level has put downward pressure on the price of submarine capacity, which declines by 25-28% per year.[105]

The result is that Big Tech influence in the SCs market extends beyond the technology sector, impacting economic and geopolitical ones. Two overarching trends emerge: first, the continuous innovation within the ICT field; second, the balance is influenced by US-China competition. Kellee Wicker stated, "***Cables are an enormous lever of power***" and "***If you can't control these networks directly, you want a company you can trust to control them.***"[106] Indeed, SubCom has become a key player in the US-China tech war to boost Washington's economic and military might. Reuters report (2023) reveals Biden administration wants SubCom to lay more SCs controlled by US companies, as a strategy to ensure that America remains the primary custodian of the Internet.[107] In this vein, SubCom's involvement in the Australia Oman cable project from Perth to Muscat, including a clandestine mission on the remote Indian Ocean Island of Diego Garcia (US Navy base), which was funded by the Pentagon to enhance surveillance on China's expansion at sea. It is noteworthy to highlight the role of India and the centrality of partnerships with the West, particularly Europe and Italy, which form a forward-looking economic and technological supply chain. This dynamic underscore a future-oriented collaboration that holds significance in the evolving landscape of global connectivity (see Section 4). Back in 2017, Prof. Thorsten Wojczewski called India an "***independent actor that stands between East and West, North and South, First and Third World.***"

3.3 Braided cables, power-tech (inter)dependencies

Examining the geographical landscape and the influence of Big Tech in the SCs market reveals a critical interplay between politics and economic development. The need for network expansion is crucial for redundancy in face of disruptions, and protecting this infrastructure is equally vital. The rupture in 2015, which isolated the Northern Mariana Islands, exemplifies the economic impact, with losses of $ 21 million for a population of 50.000, underscoring the importance of SCs resilience for both economic stability and national security.[108] Furthermore, businesses and non-governmental organizations in the market for such infrastructures cannot efficiently protect their installations without the active involvement of national security, and their scope of action is rather limited.[109]

However, there seems to be a positive correlation between cable installation and the emergence of local activities, the arrival of foreign companies and investments, and improvements in communication and connection with the global economy.[110] Research Triangle Institute (RTI) employed a different theoretical framework to explain the causal mechanisms between SCs and economic development. According to RTI, the installation of SCs enhances competition in data traffic, leading to lower Internet tariffs and increased speed. In fact, improved connectivity generates more "***Consumers' consumption of digital***

[105] Miller, Jayne. "Submarine Cables: Are We in a New Bubble?" ***Telegeography*** (2017), available at ***https://blog.telegeography.com/ptc-submarine-cable-bubble-presentation-2017-market-summary.***

[106] Brock, Joe. "Inside the subsea cable firm secretly helping America take on China." ***Reuters*** (July 6, 2023), available at https://www.reuters.com/investigates/special-report/us-china-tech-subcom/

[107] Ibidem.

[108] ESCAP, UN. "Broadband connectivity in Pacific Island countries." (2018); see also Liao, Xuexia. "Protection of Submarine Cables against Acts of Terrorism." Ocean Yearbook Online 33.1 (2019): 456-486.

[109] Morel, Camille. "La mise en péril du réseau sous-marin international de communication." ***Flux*** 4 (2019): 34-45.

[110] Hjort, Jonas, and Poulsen, Jonas. "The arrival of fast internet and employment in Africa." ***American Economic Review*** 109.3 (2019): 1032-1079.

content, products, and services," while expanding domestic market opportunities, increasing the level of competition, and creating a downward spiral for costs.[111] Consequently, political, and economic development are deeply interlinked with Internet connections, and the Organization for Economic Cooperation and Development and EU urge developing countries to follow this approach.[112] In 2014, a World Bank report indicated that "***a 10% increase in broadband penetration results in a 1.38% increase in gross domestic product (GDP) growth in low and middle-income countries.***"

Moreover, other researchers have demonstrated that connectivity reduces poverty, expands education, fosters gender equality, enhances health services, safeguards environmental sustainability, and provides a stage for international development alliances.[113] However, it is crucial for legislators to recognize that these benefits are confined to regions directly impacted by the new technology. This carries the risk of exacerbating economic and social disparities in areas that do not benefit from these advances.

The importance of understanding the socioeconomic impacts of infrastructure is becoming increasingly recognized in public policy and has attracted considerable interest among researchers,[114] examining case studies such as the Quantum Cable project, which consists of an ultra-high-speed SC linking Asia to Europe via the Mediterranean Sea and is capable of handling up to 60% of the world's Internet traffic during peak hours.[115] Like a "***huge data highway,"*** Quantum Cable connects Cyprus with Israel and Greece, then extends to Italy, France, and Bilbao, Spain, where it connects to the MAREA cable that crosses the Atlantic reaching Virginia Beach, US. Quantum Cable was laid simultaneously with the EuroAsia Interconnector and the EuroAfrica Interconnector (i.e., energy highways connecting Asia to Europe and Africa to Europe, respectively),[116] realizing scale economies. The two interconnectors to "***create a reliable alternative route for the transfer of electricity to and from Europe***" and the Quantum Cable, are opportunities for the EU to stabilize its negotiating power in the region. Cyprus as a pivotal telecom hub, in addition to its new role as a regional energy centre, transforms and upgrades its strategic geopolitical position.[117] Similarly, after the crises suffered in recent decades, Greece needs an injection of modernity and competitiveness for its domestic industries to compete globally. These countries, but also Italy and Spain, grappling with economic challenges following the global financial crisis and the European sovereign debt crisis, see this infrastructure as a strategic opportunity. Through these initiatives, nations increase their national economies in terms of both aggregate GDP growth and productivity.[118] In this line, an opportunity to expand economic ties and help Chile become a hub for data

[111] O'Connor, Alan C., Anderson, Benjamin, Lewis, Alexander C., Brower, Alice Olive, and Lawrence, Sara E. "Economic impacts of submarine fiber optic cables and broadband connectivity in South Africa." ***RTI Working Paper 0214363.202.5*** (2020), available at ***https://www.rti.org/publication/economic-impacts-submarinefiber-optic-cables-and-broadband-connectivity-south-africa/***

[112] Id. at 81.

[113] Maharaj, Sunil, and Barnes, Simon. "Better connectivity has economic spinoffs for Africa." ***The Conversation*** (2015), available at ***https://theconversation.com/better-connectivity-has-economicspinoffs-for-africa-42341***

[114] De Rogatis, Pierluigi. "The political economy of submarine cables: the quantum cable project in the Mediterranean Sea." ***The Square Insights*** 18 (2022), available at SSRN https://ssrn.com/abstract=4144465

[115] Quantum House. "Quantum Cable." ***EuroAsia Interconnector*** (2020).

[116] Interconnector, EuroAfrica. "EuroAfrica project schedule." (2020), available at: https://www.euroafrica-interconnector.com; see also: Interconnector, EuroAsia. "Trilateral Summit declares official support to 'timely implementation' of EuroAsia Interconnector." (2018), available at ***https://www.euroasiainterconnector.com/wpcontent/uploads/2018/05/20180515-Trilateral-Summit-declaresofficial-support_eng.pdf***

[117] Council of Europe. "Moneyval: Committee of experts on the evaluation of antimoney laundering measures and the financing of terrorism." (2008); see also Statista Research Department. "Cyprus: incidences of terrorism 1973-2016" ***Statista*** (2023) ; and Kazantzidou-Firtinidou, Danai, et al. "Seismic risk assessment as part of the National Risk Assessment for the Republic of Cyprus: from probabilistic to scenario-based approach." ***Natural Hazards*** 112.1 (2022): 665-695.

[118] Id. at 112.

transfer is Humboldt Cable, the first SC that will extend from South America (Chile) to Australia across the South Pacific Ocean, construction of which is started by Google in January 2024.[119]

If it is true that "***a nation's competitiveness depends on its industry's ability to innovate and upgrade,***" SCs are a prime example.[120] Increased connectivity expands interaction possibilities for businesses and capacity building for governments. Quantum Cable is a chance for the region, as it is expected to increase investor confidence, reduce costs for consumers and narrow the ICT gap between southern and northern Europe.[121]

Although SCs can simultaneously promote economic growth and international cooperation, there are political externalities for various actors, with a likely shift in the balance of power given the lobbying of private companies - which reap both economic profits and political influence due to their central role in the modern digital industry - and the defence of sovereign power from the opposing coalition, for which US and EU should forge a political and programmatic dialogue at the bloc level. Private companies are a steady presence in ownership consortia. Thus, lobbies exert some influence over the ownership of these infrastructures. As a result, countries are limiting their influence by adopting policies and maintaining greater control over submarine infrastructure by negotiating mutually acceptable solutions with companies. Competition could intensify impacting global relations, and geography could also be a penalizing factor. There could also be talk of technological dependence, a dynamic in which States rely on foreign private companies, with significant effects on their national security and ability to manage sensitive information flows. Europe's increased focus on SCs as a reaction to the embittering geopolitical context, the decision of which geographic areas to favour is also an opaque mix of commercial interests and political dynamics. These dynamics cannot be managed alone, but it is necessary and valuable that private companies and political actors worldwide collaborate to build and maintain costly, complex, and inter-country SCs for faster economic development (and beyond) not suffering from technology dependencies. Further research must promote win-win policy solutions that can improve a country's economic performance without losing political autonomy integrity and security.

[119] RHC. "Il cavo sottomarino di Google di 14.800 chilometri collegherà il Sud America all'Australia." ***Red Hot Cyber*** (2024), ***https://www.redhotcyber.com/post/il-cavo-sottomarino-di-google-di-14-800-chilometri-colleghera-il-sud-america-allaustralia/#:~:text=La%20lunghezza%20del%20cavo%20sar%C3%A0,diretti%20tra%20le%20due%20regioni***

[120] Porter, Michael E. ***Competitive advantage of nations: creating and sustaining superior performance***. simon and schuster, 2011.

[121] Cann, Oliver. "Revealed: The Digital Poverty Holding Back Global Growth and Development." ***World Economic Forum*** (2015), available at ***https://www.weforum.org/press/2015/04/revealed-the-digitalpoverty-holding-back-global-growth-and-development***;see also Marti, Luisa, and Rosa Puertas. "Analysis of European competitiveness based on its innovative capacity and digitalization level." ***Technology in Society*** 72 (2023): 102206.

4. The latest initiatives: the geopolitics of submarine cables as a strategic asset in the Mediterranean Sea

The IMEC MoU, approved in the 2023 G20 Summit in New Dehli, envisions, alongside a sea-rail line and a parallel energy network, a digital corridor based on SCs running from the Indian subcontinent to the Mediterranean via the Middle East, shaping the Indo-Mediterranean (Figure 5).[122]

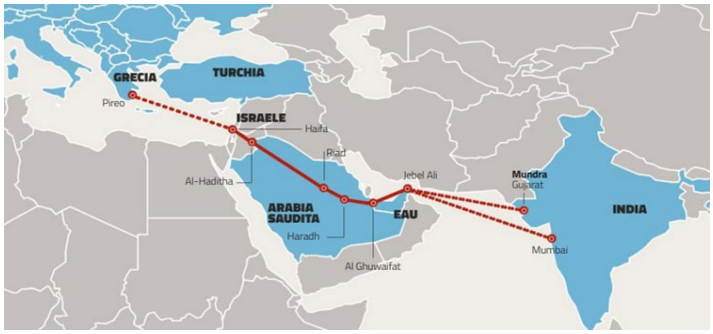

Figure. 5 – IMEC (Source: MAECI - Diplomazia Economica Italiana).

Specifically, the proposed Blue-Raman telecom cable system, built in collaboration with Google and others, will consist of two branches: a southern one, called Raman cable, will connect Jordan, Saudi Arabia, Djibouti, Oman and India, while a northern one, called Blue cable, will connect Italy with France, Greece, Israel and several countries bordering the Mediterranean Sea to Aqaba in Jordan. The latter hooks up to the new BlueMed SC from Italian Sparkle. It connects Palermo with Genoa to the rest of Europe, via Milan, and provides high-speed connectivity (Figure 6). As a new interconnection point for international digital networks, the Genoa landing platform can become the gateway for other upcoming SCs that want to enter Europe and a hub between Europe, Africa, the Middle East, and Asia.

The importance of the Italian infrastructure is evident from the ongoing negotiations between Tim and the US fund KKR for selling its network: the new arrangement includes a NetCo, which owns the network, under US-Italy control, and a ServiceCo focused on telephony operations in competition with telephone operators on the single national network.

[122] The White House. "Memorandum of Understanding on the Principles of an India – Middle East – Europe Economic Corridor." (2023), available at ***https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/09/memorandum-of-understanding-on-the-principles-of-an-india-middle-east-europe-economic-corridor/***

Figure. 6 – BlueMed Cable Map (Source: Tim Sparkle).

In geopolitical terms, the Blue-Raman cable system is the West's response to China's expansive posture, which through BRI (a.k.a. the New Silk Road) seeks to establish a hold on Eurasia; is the anchoring of India to the West through trade, military and infrastructure cooperation projects removing it from the multipolarity of the BRICS; and the involvement of Saudi Arabia, Jordan and Israel in the IMEC corridor that aims, in the medium term, to defuse the Middle East crisis and bring Tel Aviv and Riyadh closer together. This strategy is similar to that already seen during the Great Game with the British Empire within the Commonwealth as an anti-Russian function. Moreover, India, a rising power, and Italy can strengthen their bilateral relations at a time when both, which are geographically "***natural bridges***" between different regions, share a projection toward Africa and Global South and an interest in IMEC project.[123]

Italy's engagement in the region is closely linked to that of EU and NATO, with the goal of maintaining a stable presence, as envisioned by EU Indo-Pacific Cooperation Strategy, Global Gateway and NATO's Strategic Concept. In addition, Italy in order to increase its economic position in the Indo-Pacific is strengthening geo-strategic partnership with Asian countries like Japan, Vietnam and Bangladesh, is partnering with the Association of Southeast Asian Nations.[124] Through infrastructure development, the national strategy serves to promote Italian interests in trade, security, cooperation and to build resilient supply chains based on the concepts of de-risking and ***friendshoring***, leveraging EU financial and political support from US and NATO.[125] This is in a highly competitive international system in which global challenges are no longer geographically limited and need to be evaluated for their "***strategic proximity***," not just their "***geographic proximity.***"

IMEC with the Partnership for Atlantic Cooperation and the Indo-Pacific Economic Framework, is "***a visible shift from granting foreign nations market access in exchange for their geopolitical alignment to focusing on industrial policy, de-risking with China, antitrust and the creation of economic blocs.***"[126]

[123] Casini, Enrico, and Deiana, Federico. "Italia e India: tra ambizioni e interessi comuni. L'importanza di una relazione strategica." ***Fondazione Leonardo Med-Or*** (2023).

[124] Camera dei deputati. "La strategia italiana nell'indo-pacifico. Documentazione parlamentare".***Servizio Studi*** (2023) available at ***https://www.camera.it/temiap/documentazione/temi/pdf/1400847.pdf?_1702648462141***

[125] Rizzi, Alberto, and Varvelli, Arturo. "Global Gateway nel Mediterraneo: Perché l'UE deve puntare sul Vicinato meridionale." ***European Council on Foreign Relations*** (2023); see also Luciolli, Fabrizio W. "NATO's Future and the Role of Italy." ***Comitato Atlantico Italiano*** (2023).
US and NATO have a strong interest in Italy's role in the Indo-Pacific region: Italy could facilitate cooperation between EU and African Union and with I2U2 (US, India, Israel, UAE); allow US a more seamless engagement in the Pacific through a more balanced risk-sharing; strengthen dialogue and cooperation with new and existing partners in the Indo-Pacific to address interregional challenges and shared security interests of NATO. In fact, a potential crisis with Taiwan, besides depriving Western high-tech companies of 90% of semiconductors, would consistently engage the US in the Pacific, weakening US support for European security, to the advantage of the Russian Federation.

[126] Soliman, Mohammed. "Toward a Broader Atlantic Community." ***The Liberal Patriot*** (2023).

5. Conclusions

It did not take long for countries around the world to recognize that SCs were becoming a critical infrastructure for governments, the private sector, and society. There is no doubt these "***unseen and unsung cables are the true skeleton and nerve of our world, linking our countries together in a fibre-optic web.***"[127] They cross the seabed touching continents and countries, yet they go almost unnoticed by the entire planet that relies on them for many daily activities. If geopolitics deals with power struggles defined by geographical, economic, and social variables, SCs are also inherently a geopolitical phenomenon. They constitute the physical component of the digital world, delimiting its space and influencing global power by carrying increasingly crucial data. SCs remain the primary means of transporting communications and energy, providing necessary functions for our way of life. Geopolitical tensions and widespread Internet access mean that cybersecurity has become one of the most pressing concerns of the 21st century, fuelled by fears of potential disruptions that can have serious consequences for the stability of states and the continuity of global connectivity.

Our country, of course, cannot enter international consortia directly, nor is it equipped with companies that can do on their own what American or Chinese Big Tech can do, but it can implement a "***Sistema-Italia strategy,***" in which our companies are incentivized to join consortia of international companies, outline a national plan that makes our peninsula a strategic platform, interconnected with SCs both to the rest of Europe and, through Europe, to the Atlantic, and in the Mediterranean with African countries that will want to interconnect with Europe and/or with Asian countries, where the greatest production of information is expected in the coming years.[128] We should also not forget how important it is to preserve data and have digital sovereignty, firstly to ensure greater national security and, secondly, to develop the sectors of industry, research and technology, attracting international investment.

Consideration of the importance of political and industrial externalities on the economy and technology is essential, emphasizing the transfer of sovereign power and the influence of private companies in the sector. Lobbying plays a key role. At the geo-economic level, this can restructure power relations between states, intensify economic competition, and generate technological dependence and digital surveillance risk. The risk is asymmetrical economic development, with cooperative countries growing faster than those dependent on externalities. In addition, cost reduction and increased efficiency accelerate competitive dynamics.

Trends emerge: the continuous tech innovation in the telecom industry and the geopolitical impact, with the US-China geo-technological rivalry for supremacy. The role of India and partnerships with the West

[127] Assembly, UN General. "65th Sess., 59th plen." ***mtg. at 4, U.N. Doc. A/65/ PV.59*** (2010).
[128] Rossi, Emanuele. "How IMEC (and Italy) can reshape trade and ties. A conversation with Soliman." ***Decode39*** (2023).

for a future-oriented supply chain are relevant. This collaboration, crucial in the evolving global connectivity, contributes to the Energy Trilemma and enhances technological access, facilitating the growth of remote areas. G7 aims to support "***digital infrastructure for emerging and developing countries that share democratic values,***"[129] and the action plan for a "***free and open global digital infrastructure***"[130] moves in this direction. With the support of the World Bank, ITU, and private players, the expansion and control of SCs is undertaken. Italy's exit from the BRI, confirming a robust transatlantic relationship through the Indo-Pacific interest and IMEC project (which went momentarily haywire with the Oct. 7 Hamas attack), does not imply the closure of bilateral ties with China.[131] Premier Meloni's formal note confirms the desire to maintain a "***strategic friendship***" with China.[132] Given the dense network of relations between the two countries, this choice is part of a long-term vision, part of a multilateral approach, always considering the strategic alliance with the US and the current de-risking phase as part of the American geo-economic strategy,[133] this decision could bolster the competitive Italian approach in North Africa, both through the Mattei Plan and the submarine infrastructure (cf. Italian Sea Plan 2023).

Also, during the 9th Cyber Dialogue between the EU and US in Brussels, the EU Agency for Cybersecurity and the US Cybersecurity and Infrastructure Security Agency have entered a strategic partnership for the development of cyber resilience capabilities, as well as the formulation of best practices for risk management and standards in the cyber domain.[134] This agreement further solidifies a longstanding collaboration in countering cyber threats, with the hope of involving other stakeholders such as China, India, and Russia in future discussions. However, the risks are manifold: escalating tensions between the Western and Eastern blocs and, likewise, the US-China technological and informational competition; in a scenario of cyber warfare, submarine infrastructures and related chokepoints could become primary targets for government-led and proxy-state attacks, with socio-economic implications and political repercussions; data have a primary role in the competition among major powers, becoming an advantage in reshaping dynamics.

In conclusion, the question arises: ***will we witness a multilateral cooperation or power competition?*** Examining the points highlighted in the paper, it is possible to frame the issue of the SCs and power competition as part of a typical of International Political Economy scenario: the complex interdependence.[135] Given this theoretical context and the current phase of de-globalization, it is initially

[129] G7 Hiroshima Summit 2023. "Ministerial Declaration. The G7 Digital and Tech Ministers' Meeting." available at ***https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/efdaf817-4962-442d-8b5d-9fa1215cb56a/f65a20b6/20230430_news_g7_results_00.pdf***

[130] G7 Hiroshima Summit 2023. "G7 digital and tech track Annex4." available at https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/efdaf817-4962-442d-8b5d-9fa1215cb56a/d399cc87/20230430_news_g7_results_04.pdf

[131] Zeneli, Valbona. "Italy's arrivederci to China's BRI could be a template for others." ***Atlantic Council*** (2023).

[132] Galluzzo, Marco. "L'Italia è uscita dalla Via della Seta: la nota d'addio consegnata a Pechino." ***Corriere della Sera*** (2023).

[133] Rossi, Emanuele. "Così Washington pensa alla nuova geopolitica. Cosa sono Pac e Imec." ***Formiche*** (2023); see also Rossi, Emanuele. "Via dal MoU, a tutto de-risking." ***Formiche*** (2023).

[134] European Commission. "Joint Statement by United States Secretary of Homeland Security Mayorkas and European Union Commissioner for Internal Market Breton." ***EU press corner*** (2023).

[135] Buell, Raymond Leslie. ***International relations***. H. Holt, 1925; see also Nye, Joseph. "Power and interdependence: world politics in transition." ***Scott, Foresman and Company. USA*** (1977).
In contrast to the traditional realist assumptions of IPE, which place security at the center of IRs and involve the use of military force, this concept views global politics as a complex and dynamic set of specific interactions. It is defined by three characteristics: (a) a multitude of interactions connecting society, including links between governmental and non-governmental elites, formal agreements, transnational, trans-governmental, and interstate organizations; (b) the absence of a clear hierarchy in interstate relations, where military security does not consistently dominate the agenda, the distinction between domestic and foreign policy is often unclear, and specific issues necessitate and develop various links, relationships, and interactions; (c) military force is not used by governmental actors in specific regions or on certain issues when dynamics of complex interdependence prevail.

possible to respond that the geopolitical and geo-economic landscape related to the SCs may experience a power competition based on drivers such as global connectivity, access and control of information, and ultimately digital security and sovereignty.[136] In particular, the shift or redistribution of power can be driven by the role of Big Tech in owning the infrastructure and influencing political dynamics. This leads to complex scenarios in the effort to regulate global Internet architecture. Second, in the power struggles for informational competitive advantage, the country with the least technological dependence, i.e., the greatest political, economic, and technological sovereignty over the infrastructure that runs through its territory or is connected to it, such as data centres, will prevail.[137] Finally, agreements and alliances among actors united by long-lasting and highly strategic partnerships can establish power imbalances. In this latter case, the role of actors like Italy in the EU-US partnership is crucial, not only due to its geographical centrality in the Mediterranean but also because of its multilateral diplomatic approach. This makes Italy a natural chokepoint in the power relations between the two blocs, allowing for the identification of a bipolar landscape with a multipolar connotation on the infrastructure front. In such a scenario, mild forms of multilateral cooperation will emerge with the sole objective of addressing investments or, in the worst cases, preventing common threats of divergent political and financial interests and mitigating potential risks on the commercial, infrastructural, and security (not only cyber) front.

Acknowledgements

Il presente paper è stato realizzato nell'ambito del progetto "Geopolitica del Digitale", promosso dalla Fondazione Med-Or, in collaborazione con il Center for International and Strategic Studies (CISS) della Luiss Guido Carli, grazie al sostegno della Fondazione Compagnia di San Paolo all'interno del bando "Geopolitica e tecnologia."

[136] Kornprobst, Markus, and Wallace, Jon. "What is deglobalization?" ***Chatham House*** (2022), available at https://www.chathamhouse.org/2021/10/what-deglobalization
[137] Gabanelli, Milena, and Savelli, Fabio. "I dati di quasi 8 miliardi di persone passano nei cavi sottomarini. Chi li controlla?" ***Corriere della Sera*** (2020).

Additional Information

Alessandra Galassi, ***PhD Candidate in the Department of Information Engineering, Computer Science and Mathematics***, alessandra.galassi@graduate.univaq.it

Alessandra Galassi (Graduate Student Member, IEEE) is a Ph.D. Candidate in Information and Communication Technologies (ICT) at the University of L'Aquila. She has worked as an adjunct lecturer and participates in conferences. She broadened her education with a 2nd level master universitario in Cybersecurity from Luiss University and a postgraduate diploma in Economic Security, Geopolitics and Intelligence from the Italian Society of International Organization. She is listed in the Order of Engineers of the Province of L'Aquila.

Gianmarco Gabriele Marchionna, *Cyber Strategy & Technology Advisor, Researcher and Lecturer,*
ggmarchionnapro@gmail.com - gianmarco.marchionna@bip-group.com

Gianmarco Gabriele Marchionna works as a Cyber Strategy & Technology Advisor at CyberSec CoE - BIP Spa. He holds a master's degree in International Security (University of Bologna), an executive course in Strategic Affairs (LUISS School of Government), a postgraduate master's degree in Cybersecurity Management (Polytechnic of Milan), and a 2nd level master's degree in Intelligence & Emerging Technologies (University of Udine; Centre for Defense Higher Studies). He carries out teaching, research, and academic activities on topics like geo-economics, intelligence and national security, information security, AI policy, and emerging technologies.

About Luiss School of Government

The Luiss School of Government (SoG) is a graduate school training high-level public and private officials to handle political and government decision-making processes. It is committed to provide theoretical and hands-on skills of good government to the future heads of the legislative, governmental and administrative institutions, industry, special-interest associations, non-governmental groups, political parties, consultancy firms, public policy research institutions, foundations and public affairs institutions. The SoG provides its students with the skills needed to respond to current and future public policy challenges. While public policy was enclosed within the state throughout most of the last century, the same thing cannot be said for the new century. Public policy is now actively conducted outside and beyond the state. Not only in Europe but also around the world, states do not have total control over those public political processes that influence their decisions. While markets are Europeanised and globalised, the same cannot be said for the state.

The educational contents of the SoG reflect the need to grasp this evolving scenario since it combines the theoretical aspects of political studies (such as political science, international relations, economics, law, history, sociology, organisation and management) with the practical components of government (such as those connected with the analysis and evaluation of public policies, public opinion, interests' representation, advocacy and organizational leadership).

For more information about the Luiss School of Government and its academic and research activities visit. www.sog.luiss.it

May 2024

Luiss
School of Government

Via di Villa Emiliani 14
00197 Roma
T +39 85 225052
sog@luiss.it