CCSIRS | POLICY PAPER

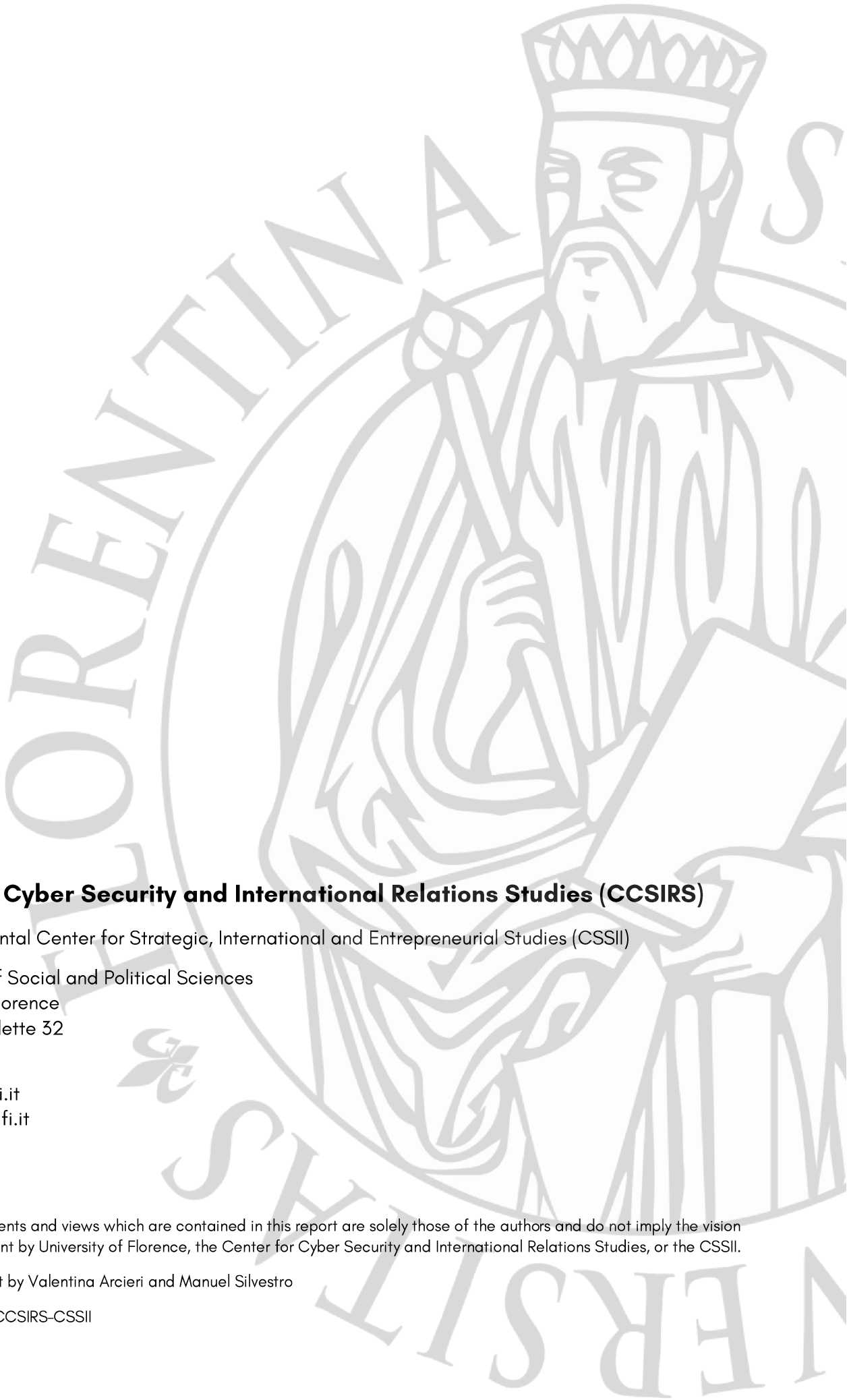
GEOSTRATEGIC VALUE OF SUBMARINE INTERNET CABLES

ITALY AS A STRATEGIC KEY POINT

Irene Spadaro
Anna Pagnacco

Center for Cyber Security and International Relations Studies

ISSUE
February 2021



Center for Cyber Security and International Relations Studies (CCSIRS)

Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII)

Department of Social and Political Sciences
University of Florence
Via delle Pandette 32
50127 Firenze

www.cssii.unifi.it
cyber@cssii.unifi.it

Design and layout by Valentina Arcieri and Manuel Silvestro

CCSIRS | POLICY PAPER

GEOSTRATEGIC VALUE OF SUBMARINE INTERNET CABLES

ITALY AS A STRATEGIC KEY POINT

Irene Spadaro

Anna Pagnacco

Center for Cyber Security and International Relations Studies

ISSUE
February 2021

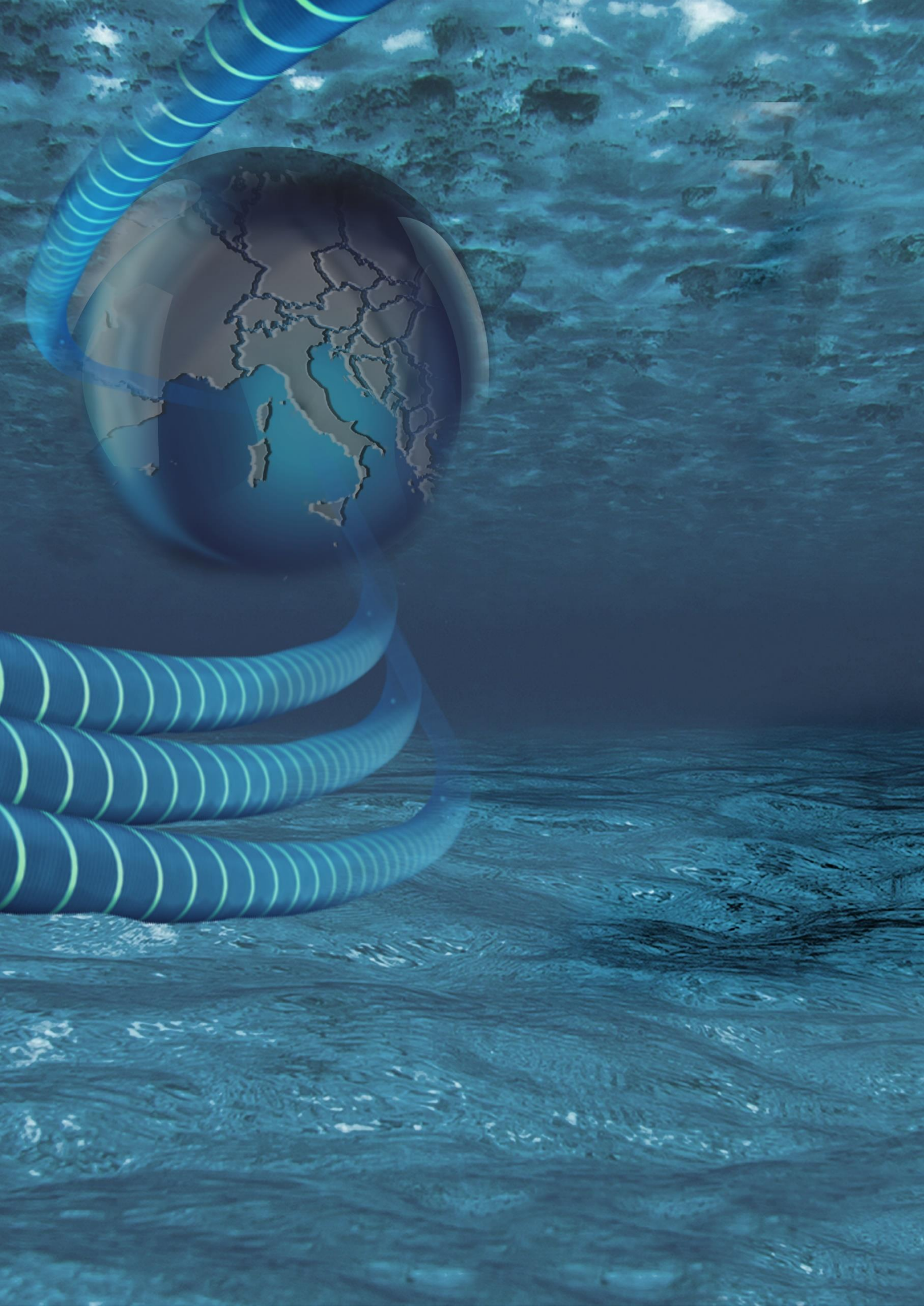
ABOUT THE CENTER

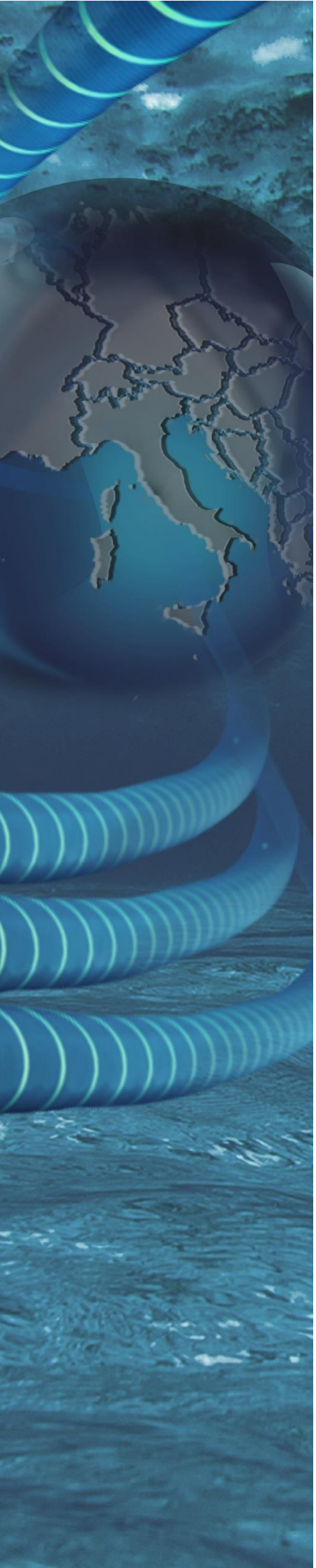
The Center for Cyber Security and International Relations Studies (CCSIRS) is part of the Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII) at the Department of Political Sciences of the University of Florence. Established in 2015, the CCSIRS aims at promoting and deepening the knowledge on cyberspace dynamics through a policy-oriented approach. More specifically, activities are focused on analyzing the influence that cyberspace exercises over both Italian national security and the international system's stability, peace and security.

The Center's multidisciplinary approach succeeds in integrating the traditional fields of Social Sciences (politics, economics, law, strategic and military studies) and Computer Science. The analyses are conducted by Italian and international experts from various sectors and countries. The Center shapes its international activities by creating an ever-increasing solid network of public and private partnerships, aiming at guaranteeing excellent research.

The Center's research focuses on comparative analysis of best cases and best practices in the fields of cyber strategy, governance and policy, critical infrastructures, economic and financial cybercrimes, privacy protection legislations and cyber intelligence structures. Complementarily, it carries out studies on the different approaches adopted internationally by both private and public actors.

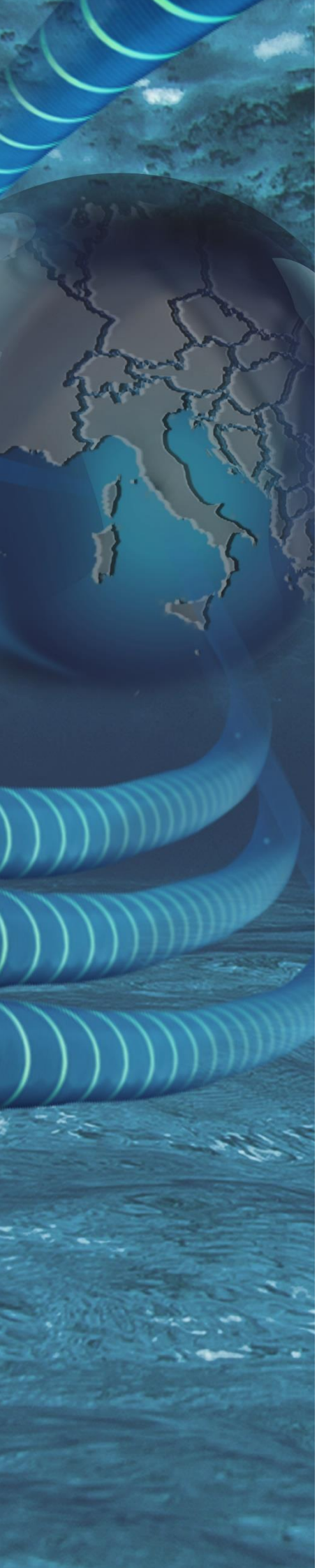
Table of contents





Executive Summary

- The global Internet is powered by thin fibre-optic cables that lie on the oceans' seabed. This infrastructure is composed of more than one million kilometres' length of cables and provides more than 95% of overall Internet connectivity, constituting the skeleton of modern financial transactions, communication and commerce system.
- Submarine cables are especially important for national security, as they are used to undertake and coordinate military operations and for gathering intelligence data; in addition, classified information oftentimes flows through the same cables of the civilian data. The general location of the cables, as well as their landing point, is a matter of public knowledge in order to avoid unintentional damage, notably increasing the potential for intentional attacks.
- The world's ability for instantaneous information sharing and communications transmission for economic and strategic purposes depends entirely on physically fragile undersea cables , whose small size is often compared to that of garden irrigation pipes. The potential for damage that lies in the disruption of undersea cables is demonstrated by a few examples of natural and voluntary disruptions that happened in the past years.
- The history of submarine cables construction and ownership has always been characterized by a race to the monopoly or a dominant position in the cable market. This leads to an ever-shifting, ever-evolving power balance in the geopolitics of cyber infrastructures, resulting in a tendency to decentralization towards BRICS countries and the Mediterranean area. Moreover, cables are inherently geopolitical, as they are built to connect locations that tend to exchange more data.
- Italy represents one of the main hubs in the key Mediterranean area, with the Sicilian Hub being one of most wired overall, constituting an important node in global connectivity. It is also involved in projects and construction of new cables, partly redefining the ownership landscape, giving the Italian government a potential strategic advantage in such a



crucial area and leaving space for a leading role in the definition of international standards on the protection of submarine cable.

- Although there is no immediate solution to eliminate concerns on the physical vulnerability of submarine cables or to easily increase political interests, some actions can be taken at national and international levels to address both challenges; this policy paper therefore aims to provide recommendations for the decision-makers and the Italian government.

Introduction

The massive diffusion of the Internet has implications on almost every aspect of our daily life, from society and economy to security and politics, both on the national and international level. Cyberspace, where the world's information flows, does not exist in a vacuum; it is not entirely virtual. It has a dual nature, consisting of a digital side and a "physical" side that includes all essential infrastructures sustaining the Internet, from the cables that carry terabits of information every second, to cable landing stations (CLS) and individual servers and computers. The whole global communication infrastructure system therefore relies upon a long chain[1] of interconnected physical cyber systems: failure or disruption of one of the parts usually results in failure or disruption of the others, affecting nations' society, economy and politics.

Specifically, the global Internet is powered by thin fibre-optic cables that lie under the oceans. This infrastructure is composed of more than one million kilometres' length of cables[2] and provides more than 95% of the overall Internet connectivity[3], constituting the skeleton of the world's financial transactions, communication, and commerce, as well as intelligence and defence communications and operations. Regardless of the fundamental role the submarine Internet cable system plays in public affairs, this infrastructure has been built over decades mainly as a result of private initiative, rather than a result of centralized state infrastructure projects akin to those backing communication and transportation pathways such as road or water networks.

Therefore, the world's ability for instantaneous information sharing and communications transmission for economic and strategic purposes depends entirely on undersea cables and their relevance cannot be underestimated. Several high-level military officials have publicly commented on the matter, so much so that Air Force Marshal Sir Stuart Peach, UK's most senior military officer, has called the vulnerability of undersea cables a "new risk to our way of life"[4] and that, according to Robert Hannigan, former director of the UK Government Communications Headquarters (GCHQ) significant disruption to the UK's economy could be brought about by cutting only a few cables. [5]

The many uses of this network and, above all, its ubiquity make it emerge as one of the most important uses of the oceans (Burnett, Davenport and Beckman 2013). And while the cable industry has been justly

[1] According to Choucri and Agarwal, a "long-chain of global communication infrastructure" is a system "characterized by distinct cyber-physical features, whose security is essential for the operation of the entire global communication infrastructure." (Choucri, Agarwal, 2019, p. 1)
[2] Submarine Cable FAQs. Retrieved 10 January 2021, from https://www2.telegeography.com/submarinecable-faqs-frequently-asked-questions
[3] Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans – Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC
[4] RUSI Whitehall. (2017). Annual Chief of the Defence Staff Lecture 2017 [Video]. RUSI Whitehall.
[5] Haynes (2017, December 04), 'Economy vulnerable to Russian attack on undersea cable', The Times, retrieved from: https://www.thetimes.co.uk/article/economy-vulnerable-to-russian-attack-on-undersea-cable-linksrqqf0fxj8

preoccupied with making the cables technically reliable,[6] they remain physically fragile by nature because of their small size, often compared to that of garden irrigation pipes.[7]

Moreover, the common idea that the Internet is mainly powered by satellites is a great misconception as, in reality, more than 95% of internet traffic runs on submarine internet cables[8], as data transfer through cables is cheaper and quicker compared to satellites.[9] Satellite transmission can be considered essential for specific uses, such as providing connection and telecommunications for sparsely populated regions not reached by cables and also as a strategic network backup for regions at high risk of natural disasters. Table I below presents a comparison of the two technologies according to a series of parameters that influence both technical and economic evaluations of investments in this sector and demonstrate which factors have led, in a free market system, to the total dependence of Internet from the state of the submarine cable network.[10]

Comparison factor	**Satellites**	**Submarine fibre cables**
Latency	250 milliseconds	50 milliseconds
Average life	10-15 years	25 years
Capacity	48.000 channels	160.000.000 channels
Unit cost per mbps of capacity	737.316$	14.327$
Percentage of traffic in 1995	50%	50%
Percentage of traffic as of 2014[11]	0.4%	99.6%

Table I. *Comparison of satellites and submarine cables to various key sectors in telecommunications* (Crain 2012, adapted from Donovan, 2009; 2014 data from FCC International Circuit Capacity Report)

In the context of the Cold War space race, satellite technology appeared to be set to dominate global communications forever. The introduction of digital optical fibre in 1988 immediately reversed this situation. The first transoceanic fibre-optic submarine cable[12] alone, at the time of its entry into service,

[6] Cable malfunctions are in most cases (72-86%) caused by external interference, and only rarely by technical failures.
[7] They can consequently be severed very easily. For their terrestrial counterparts, the intervention of squirrels is sufficient (Blum 2012); in the ocean floor, it seems that the same problem arose with sharks (Carter, 2010), probably due to their ability to perceive electric currents (Oremus 2014).
[8] Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans - Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC
[9] *Ibid.*
[10] In addition to a huge advantage in transmission efficiency, the cables are also better in other respects, such as signal quality, transmission speed, security of data transmitted, and durability once installed. (Beaufils 2000)
[11] Federal Communication Commission, International Circuit Capacity Report (2014), 3
[12] Trans-Atlantic 3 Telephone 8 (TAT-8).

had a greater capacity than all the other coaxial cables in service at that time (Beaufils 2000). And while the capacity of fibre-optic cables continues to increase, moving them further away from the limitations of their coaxial predecessors, improvements in contemporary satellites are failing to catch up. Besides, cables are unique because they have additional security and protection features that are impossible to implement in radio and satellite connections. They are stable and long-lasting and have outstanding ability and transmission efficiency.

Although they may be fragile, they also have several potential security advantages compared to other technologies for data transmission, meaning they are more efficient and suitable for classified or extremely critical data transmission, such as the management of wide-ranging weapons tests and remote war operations (Starosielski 2015). There is a network of dedicated military cables, exclusively used by heads of state and operated by military personnel mainly to ensure confidential telecommunications and direct bilateral connections between state leaders. This concentration of sensitive data however plays into the hands of espionage programs for upstream information collection, or acoustic monitoring of the seabed.[13] Undersea cables are known for being used in intelligence operations ever since the Cold War – the most famous example being the Operation Ivy Bells[14] that pioneered the use of cables as undersea communications tapping devices and, as the Snowden leaks confirmed, such practices have not ceased, meaning that submarine cables have once again proven to be a primary source of concern from an intelligence point of view.[15]

Besides, the potential for damage that lies in the disruption of undersea cables is demonstrated by a few examples of natural and voluntary disruptions that have materialized in recent years. For instance, the 2006 earthquake that hit Taiwan damaged undersea cables, cutting off internet services and phone lines and revealing the complete reliance of businesses on properly functioning Internet connection.[16] Episodes of intentional damage have also been recorded, further proving cables' potential vulnerability. For instance, in April 2009, ten fibre optic cables were deliberately and easily cut in three different locations in California, causing an interruption of 1.5 million services, including ATM and credit card processing, as well as 52,000 Verizon users' network service.[17] Even if the deliberate attacks on these

[13] SOSUS – SOund Surveillance System, v. (Weir and Center 2006)
[14] a joint effort of the Navy, CIA and NSA to listen to communications between the Soviet naval bases of Petropavlovsk and Vladivostok, on the Okhotsk Sea. Although the Soviets had installed sound detectors on the seabed and the area was continuously manned by ships engaged in military exercises, the US submarine Halibut managed to penetrate the barrier, locate the cable and, thanks to specially trained divers, install a special "bug" all around it, wrapping the cable without tearing it to prevent the enemies from noticing the intervention (De-yi, 2011). Operation Ivy Bells went on for several years, providing large amounts of data to American intelligence; it all ended when Ronald Pelton, an NSA employee, secretly leaked information to the KGB (Morris 2012). In 1981, NATO satellites showed an anomalous concentration of Soviet ships in the Okhotsk Sea, just above the point where the interception device had been located.
[15] MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian. Retrieved from https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa .
[16] The New York Times, (2006), Asia communications in chaos after earthquake off Taiwan - Asia - Pacific - International Herald Tribune, 27 December. Retrieved from: https://www.nytimes.com/2006/12/27/world/asia/27iht-quake.4032404.html
[17] Sechrist, M., 2010, Cyberspace in deep water: protecting undersea communication cables, Harvardy Kennedy School

infrastructures have been few and far between, the ability to threaten and/or protect them is increasingly crucial. As the importance of ICT technologies grows in essential infrastructures and processes such as power grids, civil and military aviation, and early warning systems, but also nuclear weapons and facilities, the use of multiple coordinated attacks can and should be expected in future conventional and unconventional conflicts.

Lastly, the history of submarine cables construction and ownership has always been characterized by a commercial and geopolitical monopolistic race for a dominant position in the cable market. This has led to a shift in power balance and the construction of a geopolitics of cyber infrastructures, that is still evolving.

This policy paper aims to partially fill in the research and policy-making analysis gap, by evaluating various dimensions of the infrastructural side of the Internet. In this view, the paper firstly provides a critical analysis of the historical and juridical framework of submarine cables. Then, the authors proceed to draw the evolving geopolitics scenarios, highlighting the role of emerging countries – notably BRICS, China, and Russia – and their relevance. Finally, the focus is directed to Italy as a strategic point framed in terms of both its strategic and geographical ecosystem and emerging national security considerations. Based on all these factors, the authors propose a series of recommendations to interested parties both in the Italian government and other stakeholders.

1. A historical and juridical framework

Submarine cables infrastructures have always been vital for governments and national security. In fact, the earliest experiences of long-distance cables were government projects aimed at military and colonial scopes: in 1858 the UK government built a submarine cable from Egypt to India via the Red Sea to allow communication regarding the "Sepoy Rebellion" unrest (Doyle 2018). The first phases of cables' evolution were characterized by a strong British hegemony, giving that the UK was the only country to have the availability of capital investment necessary and held a dominant position in global trade and colonial ventures. During the first phases of international telecommunications systems, ownership of the cables infrastructure contributed to the expansion of the UK colonial power (Headrick 1991). Contrarily, in the US, the development of submarine cables was less linked to political and security purposes, and more related to the business sector (Headrick & Griset 2001).

Since 1988, the year in which the first trans-oceanic system linking the US, UK and France was laid, around 1.2 million kilometres of fibre-optic telecommunications cables have been placed at the bottom of the oceans.[18] This only represents the latest phase in the evolution of submarine communications cables, which started in 1850 to telegraphically connect France and the UK through the English Channel. Over the first 30 years of cable construction, different private companies were created. "Of the 246,871 km of cables in place by 1892, 89.6% of the length was private and only 10.4% consisted of government cables" (Headrick 1991, pp. 58-59). World War I brought about a shift of power among States that resulted in a gradual loss of British hegemony in cable ownership; from the beginning of the XX century, in recognition of the strategic importance of submarine cables, a trend towards government control started to emerge in the United States as well. During the Great Depression commercial cable companies suffered from heavy economic losses and as a result, the maintenance and laying of cables ground to a halt. However, government-owned cables were retained due to their strategic value in a time of war, and even though since World War II global telecommunications have considerably changed, this past legacy has persisted, shaping this market as an oligopoly managed by a small group of corporations.

The main revolution in submarine cables technology came in the mid-1970s, with the development of fibre-optic cables, the first of which was laid in 1988. Not only did they play a crucial role in providing the necessary bandwidth for the development of the Internet, but the diffusion of the Internet also pushed private companies and governments to develop new technologies that helped making the Internet more accessible for a variety of users (Bartlett-McNeil 2009). These new technologies caused a spike in investment in the cables' laying and maintenance: they rose from an average of $1-2 billion

[18] Griffiths, J., (2019). The global internet is powered by vast undersea cables. But they're vulnerable. CNN. Retrieved from: https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html

per year in the 1990s to approximately $14 billion in 2000 from mainly sponsored by state-owned telecom carriers to private investments.[19] The increasing usage of the Internet by populations also contributed significantly to this investment rise. After the dot com bubble burst at the beginning of the XXI century, the industry of cable slowed down, resurging after 2008 on the other side of the world: initially, the shift regarded the Asian-Pacific market, then expanded to South America and Africa. Nowadays, developing countries and rising powers are the main investors in the Global South, followed by service providers such as Google, Facebook, and Amazon (UNEP 2009).

Historically, there have also been few proven cases of intentional and strategic disruption of submarine cables. Only hours after the declaration of war to Germany in WWI, the UK, which had a monopoly in submarine cables ownership, disrupted and tapped all five German submarine telegraph cables (Hink 2017; Sunak 2017). This gave the UK a strategic advantage, whose consequences helped shaping the outcome of the war itself. The so-called Zimmerman telegram, sent from Germany's Foreign Office to the its embassy in Mexico proposing German's support to the Latin American country if the United States had entered the war, was encrypted by British intelligence, and contributed to the involvement of the US in the War.[20] Germany on the other hand, lacking sufficient cable naval capabilities, attacked the UK landing points in the Pacific Ocean. This historic case study perfectly illustrates all the physical vulnerabilities of submarine cables that, to these days, still pose a pressing threat to their integrity: cable cutting and tapping and disruption of landing spots. During the Cold War, furthermore, the USSR cut off five different cables at large of the Newfoundland island (Hink 2017). This episode triggered a diplomatic exchange between the US and USSR, and the following controversy was managed via the norms found in the 1884 Submarine Cable Convention. [21]

1.1 Status of submarine cables in international law

In a NATO Cooperative Cyber Defence Centre of Excellence publication, von Heinegg notes that "the current legal regime has gaps and loopholes" and that "it no longer adequately protects submarine cables" (2013, p. 309). Between 1884 and 1982, the international community implemented four legal instruments on states rights and limitations on submarine cables governance: the Convention for the Protection of Submarine Telegraph Cables (1884 Cable Convention); the Geneva Convention on the High Seas and the Convention on Continental Shelf (1958); the United Nations Convention on the Law of the Sea (UNCLOS, 1982), further analysed below.

[19] TeleGeography, "Global Bandwidth Research Service: Executive Summary."
[20] Boghardt, T. (2003). The Zimmermann Telegram: Diplomacy, Intelligence and the American Entry into World War I. Working Paper 6-04, BMW Center for German and European Studies, Georgetown University
[21] The correspondence can be retrieved from: https://archive.org/stream/departmentofstat4059unit#page/556/mode/2up, p. 555-558

1. **Convention for the Protection of Submarine Telegraph Cables (1884)**. The main Convention on protection and governance of submarine cables has set a framework that still constitutes the basis of relevant international law. Its primary aim was to provide a legal framework for cables built outside the territorial waters: within territorial seas, states maintain the right to adopt and emanate laws for the protection of cables. Article 2 of the Convention outlaws intentional disruption of submarine cables or damage caused by "culpable negligence".[22] Under Article 4 and Article 5, states and cable owners are required to indemnify each other for disruption or breaking of cables and to pay for instruments sacrificed to avoid cable disruption.
2. **Geneva Convention on the High Seas and the Continental Shelf (1958).** Whilst the 1884 Convention specifically governed submarine cables, the 1958 two Geneva Conventions and the UNCLOS comprehend different aspects of the broad Law of the Sea. The Convention on the Continental Shelf ascribes rights and duties on the coastal state: in particular, regarding the submarine cables, Article 4 states that laying or maintenance of submarine cables on continental shelves could not be obstructed by the state[23], although it still maintains the right of controlling seabed resources. In the Convention on the High sea, the Art. 26 states the freedom and the right of laying cable in the high sea while considering other states rights.[24]
3. **United Nations Convention on the Law of the Sea (1982).** Whilst Articles 87, 58 and 112(1)[25] of the UNCLOS declare the freedom of high seas and the freedom to lay submarine cables, article 112(2) limits this freedom: "When laying submarine cables or pipelines, States shall have due regard to cables or pipelines already in position. Possibilities of repairing existing cables or pipelines shall not be prejudiced" (UNCLOS, Art. 79). For the purposes of mutual protection, as regards the positioning of submarine cables, each State participating in UNCLOS is required to promulgate national laws that oblige the owners of submarine cables under their jurisdiction to indemnify any damage caused to another cable by their operations (Art. 114, UNCLOS). Additionally, this right is subjected to other States' exercise of their freedom in high seas, such as navigation, and activities relating to seabed mining and other resources exploitations. According to UNCLOS, coastal and archipelagic states have the possibility to regulate any type of operations connected with submarine cables, where they do not fall within the category of "innocent passage" (Articles 18, 19 and 52, UNCLOS). They also have the right, but not the duty, to adopt and apply laws relating to the protection of cables in their territorial waters (Art. 21 (1) (c), UNCLOS). States participating in UNCLOS are required to enact legislation that criminalizes acts of breaking or damaging submarine cables committed "voluntarily or through culpable negligence" on the high seas or in the EEZs by their citizens and

[22] Convention for the Protection of Submarine Telegraph Cables, Art. 2, p. 2.
[23] Geneva Convention on the Continental Shelf, Art. 4, p. 2.
[24] Geneva Convention of the High Seas, Art. 26, p.8.
[25] Ibid., Art 112(1), p. 64.

ships flying their flag (Art. 113, UNCLOS). The result is an extension of criminal jurisdiction, normally limited to the national territory only. Fig. 1 below describes the legal delimitation stated by UNCLOS and other relevant treaties, to better grasp the status of submarine cables depending on their location.

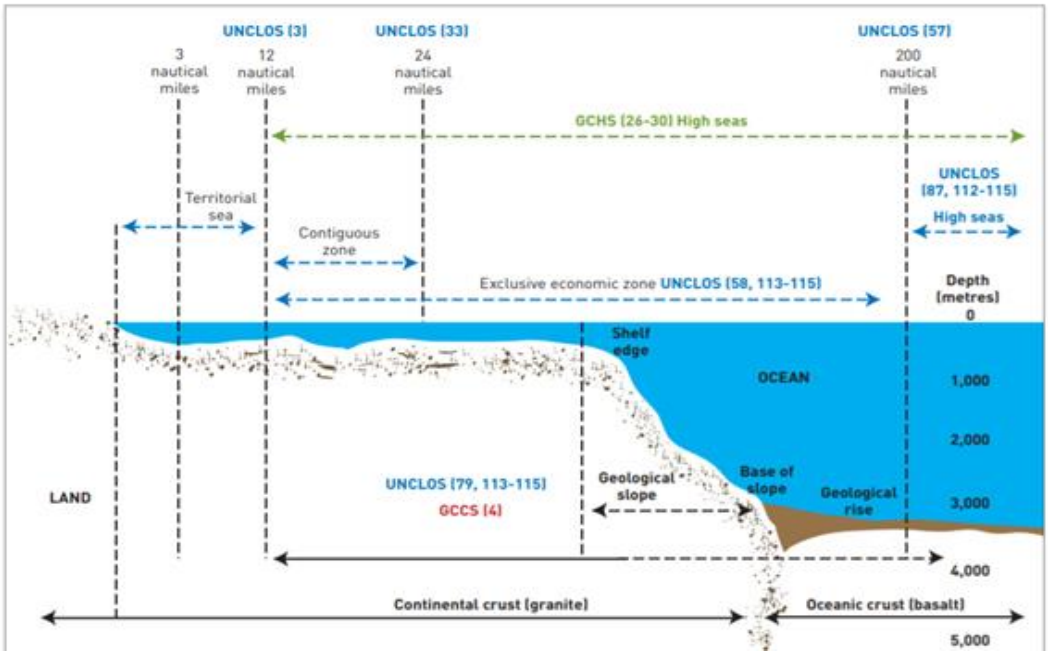


Fig. 1.: Legal boundaries of the ocean from territorial sea to exclusive economic zone and onto the high seas (figures in parenthesis refer to treaty articles). Source: D. Burnett, 2009, UNEP.

1.1.1. Challenges and ambiguity of submarine cables' status in international law

Although the status of submarine cables in international law is somehow defined, many authors and policymakers have highlighted some challenges related to the legal governance of the cable, especially as they are placed outside the jurisdiction of a state and lie at the bottom of high seas (Barker, 2018). The current regime is inadequate, both in terms of their protection in times of peace and in times of war. UNCLOS does not oblige states to establish rules and laws on the protection of submarine cables, assuming nations would recognize cables' importance and would regulate the matter. However, most states do not have sufficient legal protections in place. Strong international regulation is necessary to ensure the protection of the submarine infrastructure in international waters, but the more restrictive 1884 Convention has been only ratified by 37 states[26] whilst UNCLOS, signed by 167 states, leaves room for a generous interpretation in its application and still lacks the ratification of major countries, notably

[26] Protection of submarine cables, 1884

the U.S. Besides, the 1982 United Nations Convention on the Law of the Sea dates to before submarine cables assumed their present significance.

The 1884 Convention stated that laws on submarine cables do not "affect the liberty of action of belligerent states" in wartime (Art. 15, p. 5). Rule 37 of the San Remo Manual of Law Applicable to Conflict at Sea[27] and Article 54 of the Oxford Manual of the Laws of Naval War[28] forbid States to disrupt cables of neutral States, even if these connect the neutral state with an enemy state. Military cables, regardless of the ownership and the use for which they are intended, are subject to the same regime under international law that governs all submarine cables (Roach 2014), nor have any past conventions ever stated otherwise. However, for obvious strategic reasons their position is not public, as due to a different evaluation of opportunities, greater risk of accidental damage is balanced by the advantage of hiding an interesting target in the event of an attack.

One of the main issues arises when trying to assess whether an attack on a submarine cable, outside the jurisdiction of a state, qualifies as an "armed attack" for the purposes of Article 51 of the United Nations Charter, allowing the use of the force by a State in self-defence. According to the Tallinn 2.0 Handbook[29], the simple gathering of information from submarine cables that simultaneously transmit military and civilian data does not in itself amount to an attack as it is merely considered an act of espionage. In any case, in all controversies related to cables, the answer is always subject to the principles of proportionality and precaution, to minimize the damage to the civilian population. Moreover, given the variety and type of data transported and the services potentially involved, an assessment of damages and responsibilities could prove quite difficult. (Kraska 2020) Furthermore, regarding kinetic attacks to the submarine cable system in wartime, the Hague Regulations (1907) recognize an exception that essentially negates the rule: it outlaws the destruction of the cables during wartime, except in the case of "absolute necessity".[30] Even if the article is about submarine cables, the Convention only applies to land conflict scenarios, so it does not entail the possibility of destruction in open seas. However, following the customary law and practice of States, the cables connecting two points in the enemy territory may be cut (Tucker 1955). Therefore, while peacetime regulations are dated and exceedingly vague, international law regulating the status of the cables in wartime is even more ambiguous; the law of naval warfare is mainly customary and practice-based (Kraska 2020).

[27] Rule 37, p. 7.
[28] Art. 54, P. 8.
[29] The Tallin Manual is part of a project of NATO Cooperative Cyber Defense Center of Excellence, though it is not considered an official document of the Atlantic alliance. The Manual aims to reflect the customary international law on cyber operations and rules adopted unanimously by a group of experts.
[30] Hague Convention on laws and customs of war on land, Art. 54, p. 653.

2. Evolving geopolitical scenarios: shifts in ownership balance

Cyberspace and its infrastructures present unique features. Even though its "geography" is artificially created and modified, therefore being far more mutable than the physical components of traditional geography, it is not completely malleable, as limitations can be found in its infrastructure governance and distribution. Then, parts of cyberspace itself can be switched on and off easily and can be created and modified by routers or simple code. Framing a physical infrastructure such as submarine cables within a geopolitical context allows the decision-makers to comprehensively analyse the physical and political side of cyberspace.

Globally, the infrastructures that form the Internet and the capabilities to manufacture its components are concentrated in the hands of a few key states. While the United States is still dominant in this sector, ownership, and control of key elements of the Internet infrastructure are increasingly shifting towards the Mediterranean area, the BRICS and the rest of the world, complicating the dominant view of the US' hegemonic control over the network (Winseck 2017). This has led to rising competition between nations willing to take a leading role in the production and control of submarine cables, often following in the footsteps of old competitions and alliances patterns (Levine & Pipikaite 2019).

Ownership of international communication networks has two advantages: it provides faster and cheaper connections to states' users and services, and it allows states to maintain a competitive advantage. Connectivity also changes how much disruption can be provoked by a single accident, with developing, less connected countries suffering bigger consequences in case of destruction of single cables. In fact, smaller and less digitized countries are particularly vulnerable, because they may be dependent on a single cable for their entire Internet connectivity. This is the case of Mauritania and the ACE – African Coast to Europe cable, whose accidental break in 2018 led to the complete unavailability of the Internet in the whole country for 48 hours.[31] Similarly, Somalia in 2017 was cut off from Internet communication for three weeks because of the cable damage, with an estimated cost of 10 million dollars per day.[32] In cyberspace, contrarily, the technological backwardness of a country can paradoxically be an advantage. It is not difficult to imagine the technical consequences of an outage like the Mauritanian one in more highly digitized countries where essential services are dependent on the Internet – or the consequences of such an event during a conflict.

[31] Adepetun, A., (2020). Confusion as submarine cable cuts, slows Internet. The Guardian. Retrieved from: https://guardian.ng/news/confusion-as-submarine-cable-cuts-slows-internet/

[32] MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian. Retrieved from https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

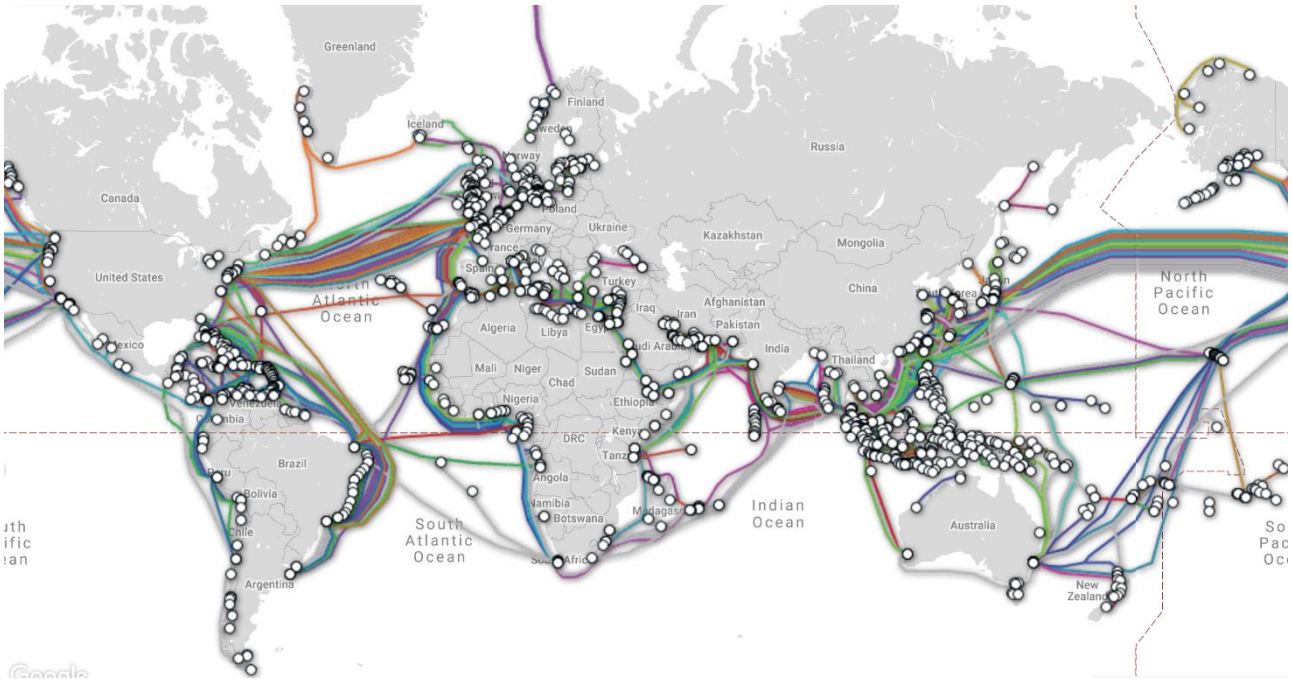


Fig. 2. Source: Submarine Cable Map (TeleGeography, 2021)

The United States is the most wired country in the world, with cables landing at both East and West Coast and worldwide connectivity. Their central position both in construction and in control of core submarine cables is coupled with a nearly monopolistic position as regards the control over cloud computing systems. Therefore, the backbones and exchange points on which the global digital arena is founded are born and developed in the United States, thus defining their role as a leading power. The second most connected country globally is the UK, mostly as a result of its role as a pioneer in laying submarine cables from the second half of the XIX century to the second half of the '900. One of the major geopolitical transformations due to cable connectivity is a shift "from a (post)colonial Eurocentric and U.S.- centric network to one that reflects current ambitions and equilibrium" (Malecki & Wei 2009, p. 375). This results in a tendency to decentralization, given that the third most connected country in the world is Senegal and that Alexandria (Egypt) is the world's most central node. Likewise, China, Russia and the BRICS are increasingly competing for a central role in submarine cable management.

2.1. The BRICS cable project and the challenge to Western hegemony

Almost half of the world population (42%) live in the BRICS countries. [33] This means that the majority of the world's users are and will be from these nations, thus bringing BRICS' cable ownership to the forefront of this geopolitical scenario. Most investments in cable construction between 2010 and 2016

[33] Nutrition and Food Systems Division. (2017). BRICS countries investing in partnerships and cooperation for nutrition-sensitive social protection. FAO. Retrieved from: http://www.fao.org/documents/card/en/c/859f9c24-74ed-485d-a652-d01adea40997/#:~:text=BRICS%20countries%20(Brazil%2C%20Russian%20Federation,percent%20of%20the%20world%27s%20population

came from the BRICS ($6.7b, or 57%), largely due to four ambitious Asia-Pacific region cable projects.[34] Edward Snowden's disclosure of the NSA and GCHQ espionage programs carried out through the tapping of submarine cables,[35] might partially be responsible for sparking interest in this infrastructure by BRICS countries. Fears of espionage pushed the group to propose the BRICS cables project: a common strategic infrastructure investment project announced in 2012, constituted of 34,000 km of cables – making it the third-longest undersea cable route globally[36] – that connect BRICS countries avoiding Europe and US hubs, with a saving up to 40% in telecommunication costs and facilitating financial transactions.[37] The cable project was based on the assumption that it should also provide more security to the group: by avoiding the Western hubs, chances of data getting intercepted or stolen noticeably decrease.

Given South Africa's major connection capabilities, the BRICS group will have direct access to other 21 African states and almost half of the world's population. In fact, South Africa is the leader in Africa's telecommunication ownership. The project, however, is stalling due to the financial and political crisis that has been affected the group in recent years[38] and not much has been publicly said on when the project intends to restart (Aouragh & Chakravartty 2016). However, single leader countries – especially Russia and China, but also to some extent South Africa and India – have been developing strategies to try and impose themselves in the race in the cable industry and management. The cable industry's eastward shift is also noted in the 2016 KPMG report "Foresight: A Global Infrastructure Perspective" as one of ten emerging trends in the Internet infrastructure, with China and India making the leap from 'emerging' markets to 'developed' markets.[39] This will give the BRICS group a strategic advantage and will partially solve their vulnerabilities related to security and geopolitical concerns.

2.2. Rising role of China in the global cables infrastructures: soft power and global influence

In this context, China's activism emerges, both as a cable supplier through Huawei Marine, and as an infrastructure buyer through state communications companies that buy cables in a consortium. Chinese actors also participate in financing projects with China Exlm Bank, which funds several projects in

[34] TeleGeography, "Global Bandwidth Research Service, Submarine Cable.
[35] MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian. Retrieved from: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[36] Sakhuja, V. (2013). BRICS: The Oceanic Connections. South Asia, 4117
[37] *Ibid.*
[38] Nordenstreng, K., & Thussu, D. K. (Eds.). (2015). Mapping BRICS media. Routledge
[39] Connolly, M. (2016). 10 emerging trends in 2016: Trends that will change the world of infrastructure over the next 5 years [Pdf]. KPMG. Retrieved from https://assets.kpmg/content/dam/kpmg/pdf/2016/03/foresight-aglobal-infrastructure-perspective.pdf#:~:text=%20%20%20Title%20%20%20Foresight%20,%20%20Created%20Date%20%20%20201603090926 58Z%20.

developing countries. It is undoubtedly the investment in infrastructure that constitutes the distinctive feature of the Chinese strategy to expand its global influence.[40] The protagonist is the company Huawei Marine, a joint venture founded in 2008 between Huawei (51%) and a subsidiary of the British Global Marine Systems (49%), active all over the world, especially in Africa.[41] China has recognized how vital it is to expand and own submarine cables infrastructures and to satisfy the demand of infrastructure of developing countries. This is because, as a 2009 World Bank report highlights, for every 10% increase in high-speed internet connection, there is a 1.3% increase in economic growth.[42] One of the results of the Chinese approach is the 2013 Belt and Road Initiative (BRI; 一带一路, yīdài yīlù) which, according to some scholars (Griffith 2017; Shen 2018), is part of China's strategy to attempt the creation of a new world order. Part of this initiative is the so-called "Digital Silk Road" (DRS), which includes building bilateral and transatlantic cables networks both for economic and strategic military purposes. The increasing investment in infrastructures is perceived as part of a wider strategy to expand China's soft power (Brake 2019) and global influence, as well as Chinese espionage and cyber security capabilities (Lee 2017). The rapid expansion of Chinese companies globally, together with Huawei's dominance in 5G wireless networks and the regulatory framework they are subject to with the constant presence of the Chinese government, raises concerns about possible security vulnerabilities, and the collection and transfer of critical information. As of now, however, China remains behind other major power cyber infrastructure capabilities: mainland China is connected by 12 submarine cables,[43] of which just 7 are owned by Chinese private telecommunications companies.[44]

The White House Telecom team blocked the project to build the Pacific Light Cable Network, a 12,800 km cable that should directly connect Los Angeles to Hong Kong. [45] This is another signal of cables' relevance in global geopolitics and the evolution of the geopolitics of cables. The US Department motivated this citing "national security" concerns as within the consortium tasked with carrying out the project, alongside the two US giants Google and Facebook, there is also Dr. Peng Telecom & Media group, the fourth telecom operator in Beijing.[46] Moreover, recently, concerns about cyber security and the possible risks of espionage led Australian intelligence to cancel Huawei's plan to link the Solomon

[40] Brake, D., (2019). Submarine Cables: Critical Infrastructure for Global Communications. Information technology & innovation foundation (ITIF).
[41] Jiang, S. (2019). China's Huawei to sell undersea cable business, buyer's exchange filing shows. Reuters. Retrieved from https://uk.reuters.com/article/uk-huawei-tech-usa-cable-idUKKCN1T40C5
[42] Qiang, C. Z., (2009). Telecommunications and Economic Growth. World Bank, Washington, DC
[43] Cable Landing Stations in China. Retrieved July 2020, from https://www.submarinenetworks.com/stations/asia/china
[44] *Ibid.*
[45] O'Keeffe, K., FitzGerald, D., (2019). National Security Concerns Threaten Undersea Data Link Backed by Google, Facebook, Wall Street Journal, 28 August. Retrieved from: https://www.wsj.com/articles/trans-pacific-tensionsthreaten-u-s-data-link-to-china-11566991801
[46] US-China row moves underwater in cable tangle. (2020). BBC News. Retrieved from https://www.bbc.co.uk/news/world-asia-53088302

Islands to Sydney.[47] Besides intelligence concerns, competitors complained that Huawei Marine would receive subsidies from the Chinese government that would allow it to sell below cost and offers contract incentives. To date, sensitive content traveling along cables is mostly protected by encryption; however, even access to metadata alone can provide potentially attractive information. Subsea network infrastructure management systems are an attractive objective for malicious activity as they allow for centralized control, creating significant security risks.

In this sense, the implementation of infrastructure technology projects in African countries creates suspicion due to the strong Chinese interests in expanding its influence in the continent. With the Digital Silk Road, China wants to introduce a new autonomous multilateral model in the governance of cyberspace, evolving from norm taker to norm shaper in the international community. Through this policy, Beijing overlooks the internal political issues of partner countries, positioning itself as an alternative to the West for the modernization and digitization of all the developing countries that would prefer not to comply with the conditions imposed by European or American infrastructure projects, especially in terms of requirements relating to the management of public power. Given the fact that the level of democratization is not a relevant criterion for joining the BRI, authoritarian governments have received, for example, highly sophisticated surveillance tools in the context of smart city projects from the Chinese government.

2.3. Russia's strategic operations on submarine cables networks

Russia is one of the main countries to have recognized the importance of cyber security and cyber weapons, as well as infrastructures' strategic centrality. There have been many episodes in which Russia demonstrated its skilful use of cyber weapons and exploitation of submarine networks' vulnerabilities for defence and intelligence purposes, but also to project its soft power potential in the geopolitics scenario.

For Russia, in order to respond to US hegemony, the BRICS submarine cable initiative proved to be inadequate: while India, Brazil and South Africa approached the project with a genuine interest in decentralized multilateral governance, on the other hand, Russia and China saw this aspect simply as a way to guarantee broad state control over the Internet. Russia is investing and improving its maritime capabilities and has a specific interest and a proven track record – as indeed the operations conducted in Crimea demonstrate - in destroying communication infrastructure as an asymmetrical method of aggression. Furthermore, in January 2014, Russia was installing what appeared to be a submarine cable across the Kerch Strait, a strait between the Black Sea and the Azov Sea, landing in the Crimean

[47] Smyth, J., (2017). Huawei's undersea cable project raises red flag in Australia. Financial Times. Retrieved from: https://www.ft.com/content/96513f58-d959-11e7-a039-c64b1c09b482

Peninsula, which has always been a strategic core node in Russian foreign policy. [48] The existence of the cable suggested that Russia was making a move to connect Ukraine's critical infrastructure with its own. In particular, it appeared that the Russian cable would carry high-speed internet communications that could bypass Ukrainian service providers (CASIS 2018). In 2015, on different occasions, US military officials and intelligence experts have warned about Russian submarines operating near cables, in its increased maritime activity.[49] Confirming these concerns, Norway has asked its NATO allies to help in detecting Russian submarines near its coasts.[50] According to the Policy Exchange report (2017) 'Undersea cables: indispensable, insecure': "Russia is using creative/hybrid warfare to overcome its hard-power disadvantages" (p. 32).

The approach with which Russia attempts to project its cyber power reflects enduring principles of the Russian approach to competition between states, extensively revised and updated due to its overall conventional inferiority. It must consider the plans and development guidelines of the armed forces of other countries and can only count on its own "intellectual superiority": hence the preference for asymmetrical and less expensive methods. However, the existence of the Yantar ship, managed by the ГУГИ – GUGI (Russian Navy's Main Directorate of Underwater Research) and officially assigned to oceanographic research activities, is in the public domain.[51] The Yantar makes it possible to operate deep-diving submarines and ROVs (remotely operated underwater vehicles) that can locate, reach, and cut a submarine cable. Such a vessel is difficult to monitor, as it can turn off or weaken its AIS signal (Automatic Identification System, an automatic tracking system used by vessel traffic services); however, it remains an eye-catching surface vessel. It is therefore more likely that it carries out reconnaissance work on the seabed for future operations and that any covert operations will be carried out by submarines. It should also be stressed that the Kremlin may be more interested in connecting interception devices to the cables that make it possible to obtain a copy of the communications transmitted.

Considering these difficulties, it seems that the current Russian strategy concerns the different and more drastic possibility of disconnecting Russia from the Internet. An exercise in this regard was recently held and hailed as a national success. Official statements have shown how authorities and telephone operators can respond to external threats to ensure the stable functioning of Runet even in the event

[48] Molodtsov, 2015, ENERGY BRIDGE «RUSSIA-ASIA PACIFIC», Ministry of energy of the Russian Federation. Retrieved from: https://www.ief.org/_resources/files/events/6th-asian-ministerial-energy-roundtable/session2--speech-by-deputy-minsiter-of-russia.pdf

[49] Sanger, D.E., Schmitt, E., (2015). Russian Ships Near Data Cables Are Too Close for U.S. Comfort. New York Times. 25 October. Retrieved from: https://www.nytimes.com/2015/10/26/world/europe/russian-presencenear-undersea-cables-concerns-us.html

[50] *Ibid.*

[51] https://lynceans.org/all-posts/you-need-to-know-about-russias-main-directorate-of-deep-sea-research-gugi/

of an attack.[52] The disconnection of the entire country at the level of submarine cables would be a particularly extreme measure, as it could also be harmful to the state itself, for example preventing important international transactions.

[52] Brzozowski, A., (2020). NATO seeks ways of protecting undersea cables from Russian attacks. Euractiv. Retrieved from: https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

3. Italy as a potential strategic key point

From previous considerations it has emerged that submarine cables are undoubtedly linked to geopolitical processes and, while the US and the UK inherited their hegemonic position from historical processes, the scenario for other countries is still evolving. China and Russia, as well as the BRICS group, are starting to take up an ever-increasing role in the cable networks arena, trying to acquire soft power and relevance in this strategic sector. It is especially challenging to properly determine the long-term impact of policies adopted in this field. There is nonetheless a place that certainly remains and could become more and more strategic: the Mediterranean Sea[53] and, along with it, Italy as a key geostrategic hub. Given the geopolitical instability of the North Africa/Middle East area, one can expect this to be an interesting space for future global dynamics.

3.1. National security considerations and the relevance of the Italian hub

Cable landing points are concentrated in two dozen sites globally, mainly located in the US and in the Mediterranean Sea: they are extremely vulnerable, being not only easily identifiable but also prone to damage caused mechanically or by natural disruptions. The authors provide a few examples to frame the cruciality of this geographic zone, intertwining them with national security considerations.

In March 2013, three divers were arrested by Egyptian naval forces as they attempted to sabotage one of the main cables, SEA-ME-WE 4, north of Alexandria. This attempt, albeit unsophisticated, caused an outage that affected several lines, reducing bandwidth in Egypt, Africa, the Middle East and Asia by up to 60%.[54] Egyptian authorities have never released any details, trying to give political explanations for what happened instead. The sabotage was painted as part of the Morsi administration's wider effort to silence domestic political dissent and media freedoms carried out with the support of the Muslim Brotherhood, while trying to shift the blame to actors such as Syria and Iran who would have sought to inflict economic damage on the Sunni Arab nations in the region to counter their support for the Syrian opposition.[55] A final effort to accuse three divers for cutting the cable could be seen as an attempt by the Egyptian government and military to divert the blame for internal economic and infrastructural failures to external forces, trying to unite the population in the face of a common threat (Maulin 2017).

[53] https://dev.networkatlas.org/
[54] Davenport, T., (2015). Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis . Catholic University Journal of Law and Technology. Vol. 24, No. 1 (December 2015): 57-109
[55] Arthur, C., (2013). Undersea internet cables off Egypt disrupted as navy arrests three. The Guardian, 28 March. Retrieved from: https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests

In 2008, a series of cables disruptions caused disservices for internet users from the Middle East, India, to the U.S.[56] This incident involved two major international cables – SEA-ME-WE 3 and SEA-ME-WE 4 – the GO-1, that links Sicily to Malta, and the FLAG FEA cable. A major unexpected repercussion was experienced by the US, particularly affecting the Defense Information Systems Agency: the cables' disservice caused a 60% loss of both commercial and military capacity in the Gulf Region, as the US military uses commercial cable networks for around 95% of its strategic communications (Sunak 2017). In 2009 Lieutenant Colonel Donald Fielden highlighted how the outage decreased UAV flights operating out of Balad Air Force base in Balad, Iraq from hundreds to tens of combat sorties per day (Sechrist 2010). It is also worth noting how the Maldives experienced a complete loss of network service because of this same disruption.[57]

Fig. 3. 2008 cables' disruption: key point, date and cable affected. Self elaboration based on various sources[58].

The situation is further complicated by the fact that repairing cables is an expensive and time-consuming practice; if the disruption is caused by a calculated and simultaneous attack on a number of crucial cables, the repair would be even more difficult to operate. In the case of the 2007 Vietnam incident, disruptions were caused by a few private citizens' attempts at salvaging cables' copper; the country's connectivity ended up depending on only one cable that, if damaged for any reason, would have left it isolated from global communication and economy.[59]

Besides cases of disruption, there is a long history of other activities such as surveillance and tapping of submarine cables. In addition to the aforementioned Operation Ivy Bells, in 1979 the USSR Parche left San Francisco in the direction of the North Pole, to place another listening device near Murmansk,

[56] CNN (2008). Third undersea Internet cable cut in Mideast. Retrieved from: https://edition.cnn.com/2008/WORLD/meast/02/01/internet.outage/
[57] Zetter, K., (2008). Undersea Cables Cut; 14 Countries Lose Web. Wired. Retrieved from: https://www.wired.com/2008/12/mediterranean-c/
[58] Icon images: Flaticon.com
[59] Ekwere, K. (2016). Submarine cables and the marine environmental: Enhancing sustainable and harmonious interactions. *China Oceans Law Review*, Vol. 2016, N. 1.

around a cable crossing the Barents Sea, where it remained undisturbed until 1992 when the wiretapping stopped (Morris 2012). Starting in 1985 the missions of the USSR Parche were extended to the Mediterranean, and in particular to the cables that connect Europe to West Africa. The submarine continued to be operative until 2004, when it was decommissioned and replaced by the USS Jimmy Carter, a US Seawolf-class submarine equipped for special missions and covert intelligence gathering housing special technicians and materials, designed for the interception of communications traveling on cables to optic fibre (Sontag & Drew 1998). As highlighted with the Snowden revelations in 2013, intrusions into communication lines (including submarine cables) no longer exclusively target classified information. Governments and spy agencies are increasingly involved in a vast scheme of information collection on the world's population; therefore, not only of content but also metadata is considered interesting thanks to advanced analytical equipment.

Characterized by rapid development since the 1990s, Europe, the Middle East and Africa (EMEA) have all seen a rise in production of submarine cable systems in recent years. This has become one of the fastest growing regions in the world, due to its scale as well as its position as a "crossroads" of the Mediterranean Sea and the Suez Canal. The EMEA region is the most consistent area in the world in terms of the actual number of systems completed. It has a growth rate that is resilient to the economic cycles pattern seen over the last 15 years. The EMEA area shows a consistent, yearly implementation of smaller regional systems, which complement larger multi-region ones, such as SEA-ME-WE. These wide projects cover different areas of the globe, rather than narrower, inter-country paths, and are the largest projects the industry is handling. As described earlier, the EMEA area is uniquely characterized as a region of steady progress, with every few years overflowing with highly ambitious regional systems, as represented by the two graphs below.

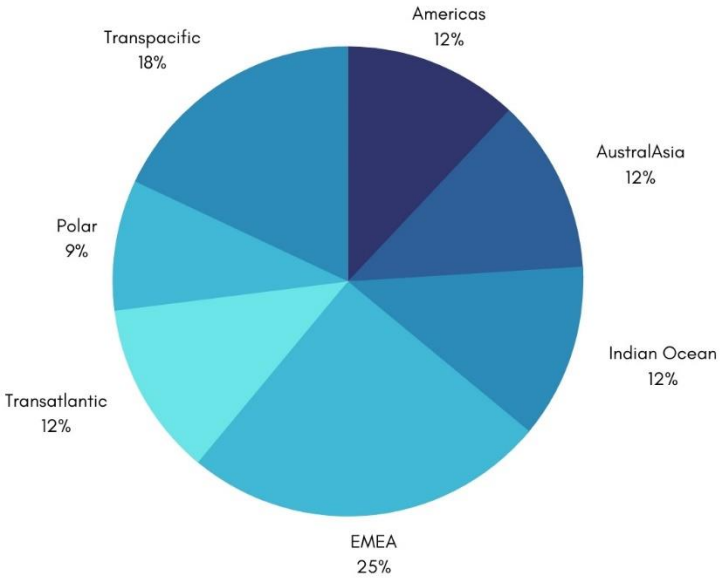


Fig.4. Planned system by region. Readadapted from: Submarine Telecoms industry report (2019)

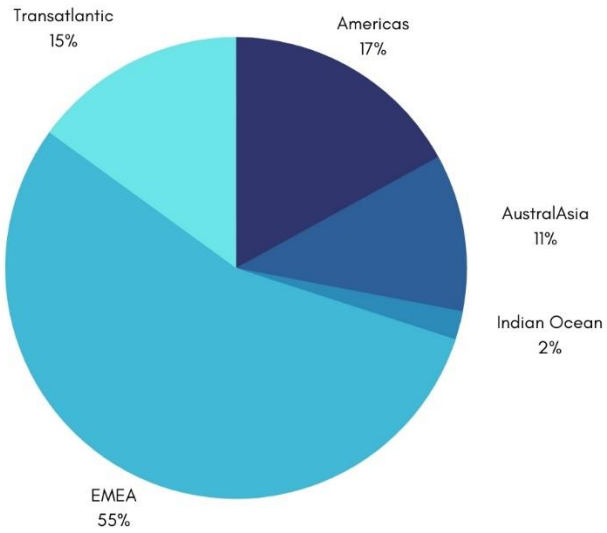


Fig. 5. Distribution of Multilateral Development Banks Investment, 2004–2019. Readapted from: Submarine Telecoms industry report (2019)

Italy, in particular, along with Egypt, constitutes one of the main hubs in the key area of the Mediterranean. Figures 6 and 7 illustrate this centrality: first, by highlighting the connections of the

Sicilian Hub – the most wired hub in the area– and then, by outlining all the landing points of the various international cables.

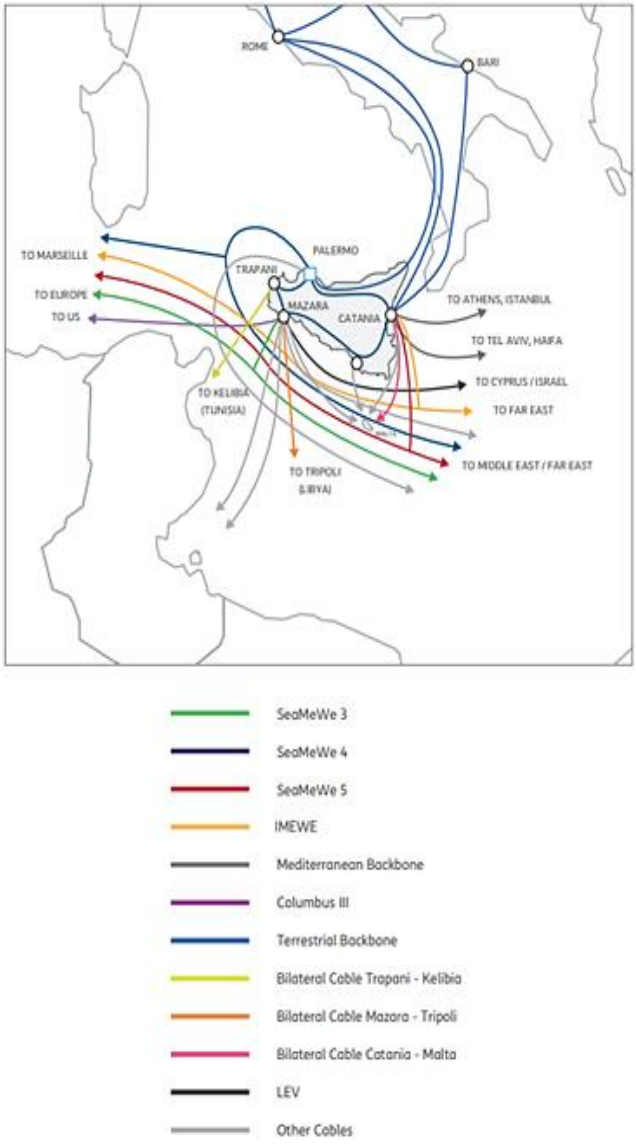


Fig. 6. Submarine Cables landing in Sicily. Source: Sparkle Group, TIM.

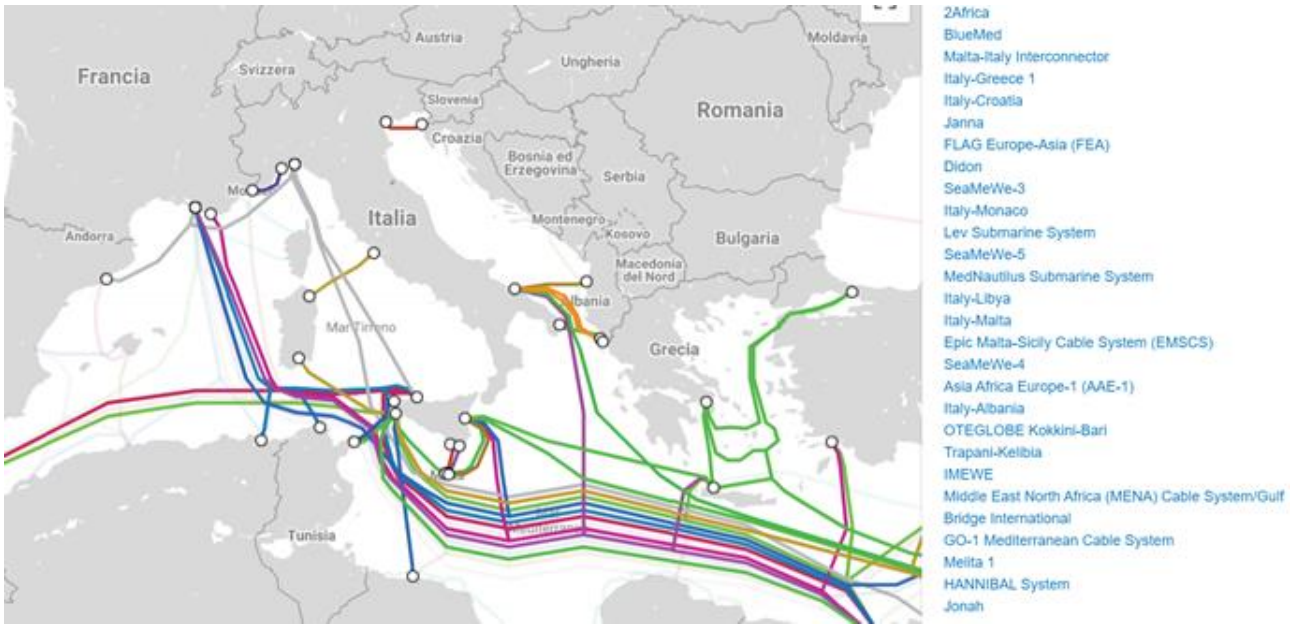


Fig. 7. Submarine Cables landing in Italy. Source: TeleGeography (2021).

Italy is also involved in recent projects and construction of new cables, partly redefining the ownership landscape. In 2015, ITALTEL, an Italian firm leader in the telecommunication sector, along with a consortium of eight shareholders, has signed a certificate of incorporation for a Sicily-based telecommunications node, aiming to become the main Mediterranean landing point (Open Hub Med – OHM) for submarine cables and the first neutral hub in Italy for the exchange of data communications.[60] The Hub was established following an approach based on principles of openness and neutrality, which is significantly different from other initiatives currently taking place in the area. Through connections between its Palermo Carini data centre, other submarine cable landing stations in Sicily and Bari, and optical fibre terrestrial paths with Milan, OHM will implement a unique international access platform offering the same neutrality, reliability, and security levels as Marseille – the only independent junction point of submarine data traffic in the Mediterranean. This initiative enabled overseas operators to diversify their data traffic routes, cutting down on submarine routes in favour of safer land paths and allowing them to benefit from reduced latency compared to the French node.[61] As stated by a spokesperson for the founding members, the Mediterranean Hub is crucial as a crossroads of submarine cables connecting India, the Middle and the Far East to Africa, Europe, South and North America, as most of the international internet data traffic and worldwide combined voice-data traffic already travels through the submarine cables in this area.

This decision was also partially a consequence of the Snowden revelations, since – as previously stated – it was disclosed that GCHQ and NSA were involved in tapping the fibre optic cables operations. In

[60] Italtel Press Release, Retrieved from: https://www.italtel.com/open-hub-internet/
[61] *Ibid.*

fact, in June 2013 the Italian weekly newspaper, L'Espresso, published allegations that the two intelligence agencies had targeted three submarine cables (SeaMeWe3, SeaMeWe4 and Flag Europe-Asia) with terminals in Sicily, intercepting commercial and military data.[62] Italian operator Sparkle, 100% owned by Telecom Italia since 2003, plays a fundamental role in the area as it manages an over-500,000 km long network of submarine fibre optic cable on which communications between Italy, the United States, North Africa, and the Middle East are transmitted. 80% of the voice and data traffic that arrives in America from the Mediterranean, including data from Google, Facebook and soon also from Amazon, transits through Italy, largely in Mazara del Vallo, one of the 5 Italian stations managed by Telecom Italia Sparkle where a total of 21 submarine cables land.[63] The main cables, mentioned before, are the SeaMeWe3 system, which arrives in Mazara del Vallo, and the SeaMeWe4 and the Flag Europe-Asia which arrive in Palermo. The SeaMeWe3, one of the longest submarine cables with its 39 thousand kilometres, has been connecting Germany to Australia since 1999, passing through Italy, Egypt, Indonesia, Philippines, Greece, India, Vietnam, China, Djibouti, Taiwan, United Arab Emirates, United Kingdom and Saudi Arabia.[64] The SeaMeWe4, installed in 2005, completes a tour of over 20 thousand kilometres connecting Marseille to Singapore and touching Italy, Egypt, Algeria, Tunisia, India, Sri Lanka, Bangladesh, United Arab Emirates, Saudi Arabia, Pakistan, Malaysia and Thailand. The Flag Europe-Asia is a 28,000-kilometer cable that since 1997 has connected the United Kingdom to Japan via Italy, Egypt, Jordan, Spain, the United Arab Emirates, Korea, China, India, Malaysia and Thailand.[65]

More cable projects involving Italy are in the works. For the construction of Google's new cable, Blu Raman – a 5,000 miles or more than 8,000 km long submarine cable that will connect Europe to India, through Israel and UAE – the firm has commissioned the construction of the first part of the cable (Blue; Genoa to Israel) to Sparkle.[66] This project is inherently geopolitical, as the same division in two "parts"' reflects a geopolitical necessity, to avoid the impression that the "Israeli" cable crosses the Saudi territory. Another point is the intentional avoidance of the construction of a hub in Egypt for different reasons: first of all because Egypt constitute the biggest single-point-of-failure, with 15 cables landing in the country which provides connectivity to almost a third of the entire world's population; secondly, because of its political instability, which does not make it the most suitable ecosystem for such a vital infrastructure; and finally, Egypt charges $300 million to lay cables across its territory, making it more expensive. Another geopolitical factor is the context of new diplomatic and commercial relations

[62] BBC, 24 June 2015. "US spy leaks: How intelligence is gathered". Retrieved from: https://www.bbc.com/news/world-us-canada-24717495
[63] Olivieri, A., 4 August 2017. "Telecom Sparkle, che cosa nasconde la rete di cavi che fece gola ad AT&T". Il Sole 24 Ore. Retrieved from: Telecom Sparkle, che cosa nasconde la rete di cavi che fece gola ad AT&T - Il Sole 24 ORE
[64] All the information on the cables can be retrieved from: https://www.submarinecablemap.com
[65] *Ibid.*
[66] Jones, R., FitzGerald, D.,23 November 2020. "Google Plans Fiber-Optic Network to Connect Via Saudi Arabia and Israel for First Time". The Wall Street Journal. Retrieved from: https://www.wsj.com/articles/google-plans-fiber-optic-network-to-connect-via-saudi-arabia-and-israel-for-first-time-11606143590

between the Gulf Arab States and Israel. Moreover, the Blue Raman cable not only will provide much more route diversity by going through Israel, but it will also decrease the cost of Asia to Europe traffic by at least 50%.

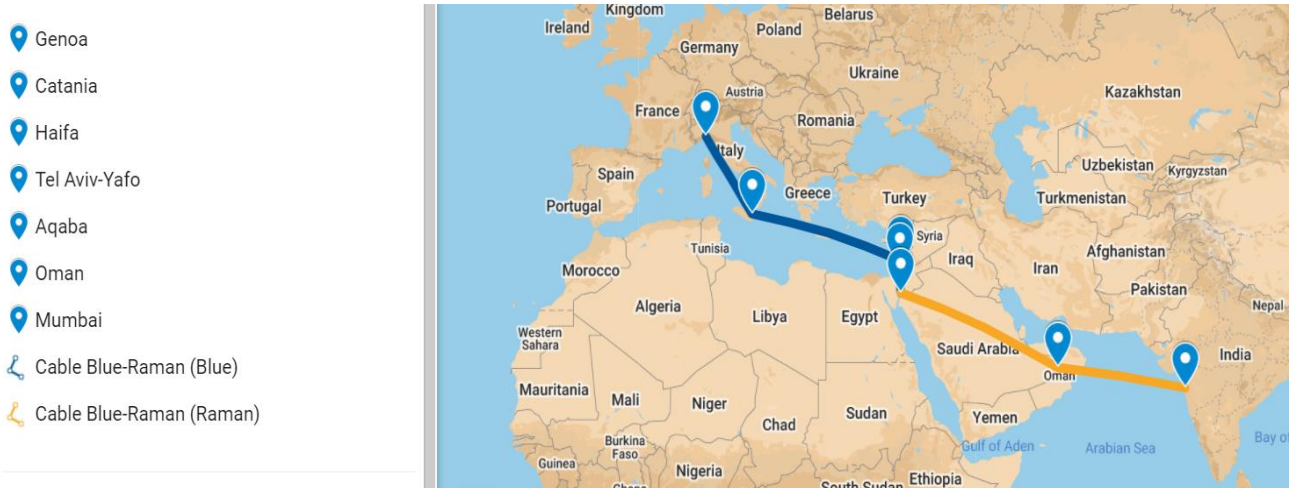


Fig. 8. Blue Raman Cable route.

At the international level, the issue has been mainly considered by NATO, coherently with its approach to cyber security governance, whilst the EU still lacks a holistic strategy on this front. The attention that the transatlantic organization has given to the cables' protection reflects its worries related to Russia's increased and prolonged undersea activities. In October 2020, NATO's defence ministers debated on the defence of submarine cables, their role as critical infrastructures and strategies to better protect this core infrastructure. NATO Secretary-General Jens Stoltenberg said members were given an assessment of threats to the submarine networks and stressed the risk of having under-protected, privately owned, and publicly located cables.[67] New tools have been put in place to protect undersea infrastructure and monitor potential threats, Stoltenberg has further explained, as the new NATO Atlantic Command in Norfolk, which monitors threats against undersea infrastructure. [68]

[67] Brzozowski, A., 23 October 2020. "NATO seeks ways of protecting undersea cables from Russian attacks".Euractiv. retrieved from: https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

[68] NATO Official statement, 22 October 2020. Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_178946.htm.

Conclusion and recommendations

Traditional geopolitics dealt with geography as a fundamental element for establishing the possibilities of movement of armies and for the necessary supply lines, for the possibility of establishing commercial traffic by sea and by land, defensible simply and inexpensively. In the digital age, geopolitics must also deal with telecommunications networks, submarine cables, hubs and landing points through which internet traffic passes and cyber attacks on critical infrastructures that may be able to bring an entire country to its knees. These scenarios can shift the modern spheres of influence and shape most of the world's commercial ventures. This new virtual geography, therefore, exerts a notable impact on decisions formulated by policymakers, who must face this ever-evolving international reality. The infrastructure of the Internet, crossing national borders, tends to overlap with historical, cultural, economic agreements or rivalries, and to favour (or disfavour) new subjects and political aspirations. For most countries, competing internationally in the Information Technology sector, although not trivial in terms of commitment and investments, is easier than trying to establish themselves in more "traditional" geopolitical confrontation arenas: this is not only due to lower overall costs but also to the intrinsic uncertainty in the process of innovation, which guarantees a chance to push back against the hegemon through intellectual work.

Every technology becomes a critical infrastructure when fundamental activities of daily life depend on it and in the twenty-first century the Internet fully satisfies this criterion. As critical infrastructures, submarine cables allow it to function properly and guarantee the continuation of international trade and defence operations; cables' safety, continuity and availability are therefore an absolute priority. Their ubiquitous nature and their increasing use for political and military purposes, combined with an almost complete absence of protective measures, poses significant risks to international peace, stability, and security. The multiplication of targets that need protection in the cyber domain disperses the energies of defensive actors against enemies virtually impossible to identify with certainty.

The vulnerability of the cables that cross the seabed constitutes an important threat to the global economy as well as society in a broader sense. In the scenario in which these cables were to be cut or their functioning in any way impaired, the effects on the world economy and the daily life of the population involved would be immediate and potentially catastrophic. If the world's 475 submarine cables were to suddenly disappear, satellites would only be able to carry a tiny fraction of global Internet traffic, and the Internet would effectively be divided into continents. Whether or not a state actor intends to isolate an area of the planet from the rest of the world, the vulnerability of submarine cables provides an extremely effective and damaging mode of action to eliminate most fundamental international communication routes with minimal effort, especially in times of crisis. The combination of minimal attention and important consequences that characterizes this infrastructure makes it an ideal

target for operations aimed at destabilizing a country's Internet connection, especially in locations constituting fundamental nodes in the Net.

Even if submarine cables could appear to be completely irrelevant, continuing to hide this physical side of the digital world from public opinion not only does not only hinder attempts to protect them from damages: in fact, it could actually end up damaging cables and their users. If cables continue to remain invisible to policymakers, governmental, private and political actors, infrastructural decisions in this sense will continue to be neglected and policy choices misinformed, with deleterious consequences on the overall stability of the network. Bringing attention to key infrastructures, usually neglected by the media and public debate, inevitably brings along two main issues: the scarcity of available information on the one hand and the Streisand effect[69] on the other. If it is precisely because of the strategic criticality of this infrastructure that it is not mentioned more frequently, a discussion of its vulnerabilities might end up further exposing it to the very risks oblivion is supposed to protect them from. However, security through obscurity is only a convenient security trade-off on rare occasions, such as the protection of secret military installations;[70] most other infrastructures are better off benefitting from the wider security community's testing and oversight. It logically follows that one should try to analyse and draw as much attention as possible to all potential risks and vulnerabilities concerning submarine cables.

Although there is no immediate solution to solve all concerns about the physical vulnerability of submarine cables and the lack of political interests, some actions can be taken to improve the situation at national and international levels:

- The shortcomings in regulation and policies on submarine cables often derive from a lack of knowledge and a lack of interest in this infrastructure. In recognizing its critical importance, countries can take various initiatives to ensure greater protection of submarine telecommunications cables. The difficulties in the management and protection of submarine cables as critical maritime infrastructure are especially aggravated by the generalized absence of competent authorities on the matter at the national level. All states should adopt clear governance frameworks for the protection of submarine cables and landing stations, as well as operative plans for catastrophic cable outages, since as of today no such coordinated mitigation plan exists nor have adequate defence-in-depth systems been put into place. Given the international and geostrategic nature of this critical infrastructure, highlighted in the

[69] A social phenomenon that occurs when an attempt to hide, remove, or censor information has the unintended consequence of further publicizing that information.
[70] And in fact, consistently with the previous statements, neither the position nor the number of cables that make up the network of submarine cables owned and used exclusively by the military are in the public domain. (Roach 2014).

previous sections, all these measures should be put in place and harmonized at a supranational level, as any country without malicious intent would benefit from it.

- The absence of both an international coherent regulatory framework and a supranational mechanism of decision making entails the adoption of fragmented policies with no strategic dimension, simultaneously damaging the industry, the states involved, and the international community in a broader sense. Since most state actors have not anticipated or even fully understood the relevance of this network and its nature as a fundamental component of international communications, the policies in this regard risk being neglected as they do not fully belong to the mandate of any institution or being contradictory following the application of provisions coming from different bodies of equal competence. The competent authorities for technological regulation, such as those dealing with standards in telecommunications, licensing of arrival stations and problems relating to competition and antitrust, may not be familiar with maritime matters. Similarly, maritime organizations that manage the latter generally ignore the nature and importance of cyberspace and the crucial role of cyberspace. To guarantee that this infrastructure is adequately protected, it is therefore fundamental to ensure a coherent approach to the topic by clarifying competent organisms at a national and international level and training them specifically to be able to fully grasp this infrastructure's implications.

- The achievement of complete redundancy in this system is of critical importance. While smaller, less connected countries whose connectivity depends on a smaller number of cables are more at risk in case of attack, they also tend to be less economically and technologically developed. Therefore, paradoxically, larger, more advanced and better-connected nations risk more in case of cable disruptions because of the contemporary tendency to digitize all sectors of public and private life. Catastrophic failures in countries such as Italy would be harder to provoke, but they would imply bigger overall and global losses as there is simply so much more at stake.

- The absence of an intergovernmental organization responsible for cables is again a symptom of the lack of interest in this issue and the cause of indifference regarding international issues relating to submarine cables. States need to adopt appropriate legislation and private actors need to raise awareness, especially where a lack of political interest in protecting this infrastructure makes it difficult to sign a treaty to protect submarine cables. As previously stated, the different approach of global actors to the management and use of this infrastructure, create a complex situation in which the creation of an intergovernmental organization seems almost impossible. To solve this impasse, relevant regional actors – such as Italy – should

encourage and promote the creation of such an organization as a basic first step which would be beneficial to their interests and overall security.

- Major cable providers (tier one providers) are private companies, further complicating the geopolitical scenario by multiplying the number of involved actors. Companies enjoy a high degree of plausible deniability whereby they can claim they are pursuing autonomous economic interests that are not clearly linked to any government, but their operative headquarters are inevitably located on a territory and therefore subjected to its jurisdiction. One wonders whether the current model of Internet governance – a multi-stakeholder model that commercial interests, technical experts, non-governmental organizations, as well as the United States and Western democracies themselves advocate – will be eroded in favour of a more state-centred multilateral system, promoted by those countries critical of US power and commercial interests. Regional Western organizations should strive to offer an alternative model of governance, in which both private and state actors are regulated, and should promote it globally.

- Regarding the legal governance of submarine cables, it is also fundamental to find an equilibrium between the international protection and regulations with state sovereignty and domestic security. This task is complicated by the fact that cable ownership is mostly private. The infrastructures' components are both located in the sovereign territory of the State and, at the same time, part of the global Internet; doubts could be raised on whether submarine cables or telecommunications satellites can be defined as a *res communis* and any attempt at analysing them should clearly distinguish the element in which they operate (water, air, space, terrestrial), the physical infrastructure, and the activity that is conducted through the infrastructure. Tapping of submarine cables to steal sensitive data that flows through it can constitute a violation of a state's sovereignty, if this is conducted in its territorial waters,[71] but it would not be a violation of the state that owns such a cable, creating dangerous opportunities.[72] States should establish boundaries and principles in international fora to solve this normative incoherence by providing a regulative framework that could work in time of crisis, both on the private and public perspective. In this sense, these types of initiatives should be promoted by states with strong interests at stake and/or a prominent position which makes them more vulnerable to intentional attacks.

- NATO should also intensify its effort to protect submarine cables from malicious activities, with special regard to Russian activity. The possibility of a direct attack aimed at damaging cables,

[71] CCDCOE, 2019, Strategic importance of, and dependence on, undersea cables, NATO CCDCOE Strategy and Law Branch.
[72] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rule 4, p. 17.

especially on a large scale, while unlikely according to most accredited geopolitical assessments, might be carried out with unsettling ease. It is therefore not excluded that, in the best Russian tradition, in case the friction with the hegemon or with other local realities intensifies, outages could ensue, isolating even large areas of the planet for long periods and considerably complicating situations of crisis or conflict. The unity of the network is indeed dependent on the unity of the network of cables that connect the continents. The control of this infrastructure will be an important area of confrontation for the world powers; the forms and contents of the Internet of the future will depend on it, as do the developments and imposition of technological standards and digital regulation.

- Working to solve the absence of political interest and public pressure regarding accountability in this area should also be a priority. First, it is necessary to sensitize the world's public opinion to the now solidified dependence, especially in developed countries, on the Internet, especially in those critical sectors upon which national security depends, and its physical vulnerabilities. A more developed collective awareness in this sense should spark renewed interest in the network that allows the Internet to exist, constituting an excellent basis for a deeper appreciation of the importance of cables.

- The majority of cable damages are due to natural causes and therefore by definition they are not attributable to any actor and are compensated thanks to private insurance coverage. However, this does not mean that they are completely beyond the reach of any policy action: for example, the frequency of environmental events damaging cables could in fact increase as extreme weather conditions due to climate change intensify. The problem should be addressed as part of the more comprehensive strategies put in place against environmental change, given how cables are one of the most essential infrastructure for the world's society, economy and security.

- Although all the recommendations given should be considered by every government and relevant regional and international organizations, these are even more pressing for highly wired States such as Italy. Its geographic location, its recent partnerships and national security concerns define a picture of particular fragility on one hand and strategic advantages on the other. As a consequence, the Italian government should take steps to protect this infrastructure to further incentivize its emerging role in the cables' market and geopolitical scenario.

- Insofar as establishing an international body dedicated to undersea cable protection is not a viable option, Italy should rise to the challenge and protect its geopolitical interests via the

promotion of a regional competent organization, especially considering previous analysis highlighting the criticality of the Mediterranean Hub. Although this area is characterized by profoundly different State actors and interests, the Italian government could start by engaging with different public and private partners to partially solve this discrepancy, creating the basis of long-term partnerships and, in the future, a multilateral initiative. Moreover, since the EMEA region continues to be characterized by economic uncertainty and political instability, casting a cloud over any prospective projects, Italy has the possibility to become the leader and the most-wired hub in this ever growing area. This could give Italy a strategic economic advantage and a hegemonic geopolitical position, accompanied by the responsibility to promote aforementioned regional and international actions.

Bibliography

Adepetun, A., (2020). Confusion as submarine cable cuts, slows Internet. The Guardian. Retrieved from: https://guardian.ng/news/confusion-as-submarine-cable-cuts-slows-internet/

Aouragh, M., & Chakravartty, P. (2016). Infrastructures of empire: Towards a critical geopolitics of media and information studies. *Media, Culture and Society*, 38(4), 559–575.

Arthur, C., (2013). Undersea internet cables off Egypt disrupted as navy arrests three. The Guardian, 28 March. Retrieved from: https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests

Barker, P. (2018). Undersea Cables and the Challenges of Protecting Seabed Lines of Communication. *Center for International Maritime Security*. Retrieved from: http://cimsec.org/underseacables-challenges-protecting-seabed-lines-communication/35889.

BBC, 24 June 2015. "US spy leaks: How intelligence is gathered". Retrieved from: https://www.bbc.com/news/world-us-canada-24717495

BBC, 24 June 2015. "US spy leaks: How intelligence is gathered". Retrieved from: https://www.bbc.com/news/world-us-canada-24717495

Boghardt, T. (2003). The Zimmermann Telegram: Diplomacy, Intelligence and the American Entry into World War I. Working Paper 6-04, BMW Center for German and European Studies, Georgetown University

Brake, D., (2019). Submarine Cables: Critical Infrastructure for Global Communications. Information technology & innovation foundation (ITIF).

Brzozowski, A., (2020). NATO seeks ways of protecting undersea cables from Russian attacks. Euractiv. Retrieved from: https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

Burnett, D. R., Beckman, R., & Davenport, T. M. (Eds.). (2013). *Submarine Cables: the handbook of Law and Policy*. Martinus Nijhoff Publishers.

Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans – Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC.

CASIS, (2018). Russian Deep-Sea Operations and Canadian Cybersecurity Issues. *The Journal of Intelligence, Conflict, and Warfare*, 1(2), 6-6.

CCDCOE, (2019). Strategic importance of, and dependence on, undersea cables, NATO CCDCOE Strategy and Law Branch

Clark, B. (2016). Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists*, 72(4), 234-237.

Clark, B. (2016). Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists*, 72(4), 234-237.

CNN (2008). Third undersea Internet cable cut in Mideast. Retrieved from: https://edition.cnn.com/2008/WORLD/meast/02/01/internet.outage/

Coffen-Smout, S., & Herbert, G. J. (2000). Submarine cables: a challenge for ocean management. *Marine Policy*, 24(6), 441-448.Costigan, S. S., et al., (2016). *Cybersecurity: A Generic Reference Curriculum*, NATO.

Connolly, M. (2016). 10 emerging trends in 2016: Trends that will change the world of infrastructure over the next 5 years [Pdf]. KPMG. Retrieved from https://assets.kpmg/content/dam/kpmg/pdf/2016/03/foresight-aglobal-infrastructure-perspective.pdf#:~:text=%20%20%20Title%20%20%20Foresight%20,%20%20Created%20Date%20%20%2020160309092658Z%20.

Davenport, T., (2015). Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. *Catholic University Journal of Law and Technology*. Vol. 24, No. 1 (December 2015): 57-109.

De-yi, M. A. (2011). The US Espionage Activity in the Sea of Okhotsk in 1970s. In *Northeast Asia Forum* (No. 2, p. 3).

Doyle, M. (Ed.). (2018). *The British Empire: A Historical Encyclopedia* [2 volumes]. ABC-CLIO.

Ekwere, K. (2016). Submarine cables and the marine environmental: Enhancing sustainable and harmonious interactions. *China Oceans Law Review*, Vol. 2016, No. 1.

Federal Communication Commission, International Circuit Capacity Report (2014), https://www.fcc.gov/reports-research/reports/international-circuit-capacity-reports/international-circuit-capacity

Griffiths, J., (2019). The global internet is powered by vast undersea cables. But they're vulnerable. CNN. Retrieved from: https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html

Haynes (2017, December 04), 'Economy vulnerable to Russian attack on undersea cable', The Times, retrieved from: https://www.thetimes.co.uk/article/economy-vulnerable-to-russian-attack-on-undersea-cable-linksrqqf0fxj8

Headrick, D. R. (1991). *The invisible weapon: Telecommunications and international politics*, 1851-1945. Oxford University Press on Demand.

Headrick, D. R., & Griset, P. (2001). Submarine telegraph cables: business and politics, 1838-1939. *The Business History Review*, 543-578.

Hinck, G. (2018). Evaluating the Russian Threat to Undersea Cables. *Lawfare*, March, 5.

International Institute of Humanitarian Law. (1995*). San Remo manual on international law applicable to armed conflicts at sea*. Cambridge: Cambridge University Press.

International Institute of International Law, (1913). *Manual of the Laws of Naval War, Oxford*, 9 August 1913, United Nations.

International Law Commission, (1958). *Convention on the Continental Shelf*, 29 April 1958, United Nations.

International Law Commission, (1958). *Convention on the High Seas*, 29 April 1958, United Nations

Jiang, S. (2019). China's Huawei to sell undersea cable business, buyer's exchange filing shows. Reuters. Retrieved from https://uk.reuters.com/article/uk-huawei-tech-usa-cable-idUKKCN1T40C5

Jones, R., FitzGerald, D.,23 November 2020. "Google Plans Fiber-Optic Network to Connect Via Saudi Arabia and Israel for First Time". The Wall Street Journal. Retrieved from: https://www.wsj.com/articles/google-plans-fiber-optic-network-to-connect-via-saudi-arabia-and-israel-for-first-time-11606143590

Kraska, J., (2020). Submarine Cables in the Law of Naval Warfare, *Lawfare*. Retrieved from: https://www.lawfareblog.com/submarine-cables-law-naval-warfare.

Levine, E., Pipikaite, A., (2019). Hardware is a cybersecurity risk. Here's what we need to know, *World Economic Forum*.

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian. Retrieved from https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian. Retrieved from https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian. Retrieved from: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Malecki, E. J., & Wei, H. (2009). A wired world: the evolving geography of submarine cables and the shift to Asia. *Annals of the Association of American Geographers*, 99(2), 360-382.

Maulin, A., (2017). Cable Breakage: When and How Cables Go Down?, 3 May. *The Huffington Post*. Retrieved from: https://www.huffingtonpost.com/daniel-nisman/who-cut-egypts-internet_b_2974208.html?guccounter=1

McGuinness, D., (2017). How a cyber attack transformed Estonia. BBC. Retrieved from: https://www.bbc.com/news/39655415#:~:text=On%2026%20April%202007%20Tallinn,in%20some%20cases%20lasted%20weeks.&text=%22Cyber%20aggression%20is%20very%20different,kinetic%20warfare%2C%22%20she%20explained.

Molodtsov, 2015, ENERGY BRIDGE «RUSSIA-ASIA PACIFIC», Ministry of energy of the Russian Federation. Retrieved from: https://www.ief.org/_resources/files/events/6th-asian-ministerial-energy-roundtable/session2--speech-by-deputy-minsiter-of-russia.pdf

Morris, C. (2012). *Operation IVY BELLS: Lessons learned from an'intelligence success*'. Journal of the Australian Institute of Professional Intelligence Officers, 20(3), 17.

Nakashima, E., (2018). Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. The Washington Post. Retrieved from: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

Nordenstreng, K., & Thussu, D. K. (Eds.). (2015). Mapping BRICS media. Routledge

Nutrition and Food Systems Division. (2017). BRICS countries investing in partnerships and cooperation for nutrition-sensitive social protection. FAO. Retrieved from: http://www.fao.org/documents/card/en/c/859f9c24-74ed-485d-a652-d01adea40997/#:~:text=BRICS%20countries%20(Brazil%2C%20Russian%20Federation,percent%20of%20the%20world%27s%20population

O'Keeffe, K., FitzGerald, D., (2019). National Security Concerns Threaten Undersea Data Link Backed by Google, Facebook, Wall Street Journal, 28 August. Retrieved from: https://www.wsj.com/articles/trans-pacific-tensionsthreaten-u-s-data-link-to-china-11566991801

Olivieri, A., 4 August 2017. "Telecom Sparkle, che cosa nasconde la rete di cavi che fece gola ad AT&T". Il Sole 24 Ore. Retrieved from: Telecom Sparkle, che cosa nasconde la rete di cavi che fece gola ad AT&T - Il Sole 24 ORE

Polityuk, P., (2017). Ukraine points finger at Russian security services in recent cyber attack. Reuters. Retrieved from: https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P

Qiang, C. Z., (2009). Telecommunications and Economic Growth. World Bank, Washington, DC

Rattray, G. J. (2009). An environmental approach to understanding cyberpower. *Cyberpower and National Security*, 253, 274.

RUSI Whitehall. (2017). Annual Chief of the Defence Staff Lecture 2017 [Video]. RUSI Whitehall.

Sakhuja, V. (2013). BRICS: The Oceanic Connections. South Asia, 4117

Sanger, D.E., Schmitt, E., (2015). Russian Ships Near Data Cables Are Too Close for U.S. Comfort. New York Times. 25 October. Retrieved from: https://www.nytimes.com/2015/10/26/world/europe/russian-presencenear-undersea-cables-concerns-us.html

Schulze, E., (2019). Russia just brought in a law to try to disconnect its internet from the rest of the world. CNBC. Retrieved from: https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html

Sechrist, M. (2010). Cyberspace in deep water: Protecting undersea communication cables by creating an international public-private partnership. Harvard Kennedy School, 20

Sechrist, M., 2010, Cyberspace in deep water: protecting undersea communication cables, Harvardy Kennedy School

Smyth, J., (2017). Huawei's undersea cable project raises red flag in Australia. Financial Times. Retrieved from: https://www.ft.com/content/96513f58-d959-11e7-a039-c64b1c09b482

Sontag, S., Drew, C., & Drew, A. L. (1998). *Blind man's bluff: the untold story of American submarine espionage*. Public Affairs

Starosielski, N. (2015). *The undersea network*. Duke University Press.

Sunak, R. (2017). *Undersea cables: indispensable, insecure*. Policy Exchange.

TeleGeography, "Global Bandwidth Research Service". Submarine Cable.

The New York Times, (2006), Asia communications in chaos after earthquake off Taiwan - Asia - Pacific - International Herald Tribune, 27 December. Retrieved from: https://www.nytimes.com/2006/12/27/world/asia/27iht-quake.4032404.html

Tucker, R. W. (1955). Rules Governing Weapons and Methods of Naval Warfare. *International Law Studies*, 50(1), 16.

U.S. Image Plummets Internationally as Most Say Country Has Handled Coronavirus Badly, 2020, Pew Research Center. Retrieved from: https://www.pewresearch.org/global/2020/09/15/us-image-plummets-internationally-as-most-say-country-has-handled-coronavirus-badly/

UN General Assembly, *Convention on the Law of the Sea*, 10 December 1982, available at: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

US-China row moves underwater in cable tangle. (2020). BBC News. Retrieved from https://www.bbc.co.uk/news/world-asia-53088302

Winseck, D. (2017). The geopolitical economy of the global internet infrastructure. *Journal of Information Policy*, 7, 228-267.

Zetter, K., (2008). Undersea Cables Cut; 14 Countries Lose Web. Wired. Retrieved from: https://www.wired.com/2008/12/mediterranean-c/

Center for Cyber Security and International Relations Studies (CCSIRS)

Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII)

Department of Social and Political Sciences
University of Florence
Via delle Pandette 32
50127 Firenze

www.cssii.unifi.it
cyber@cssii.unifi.it