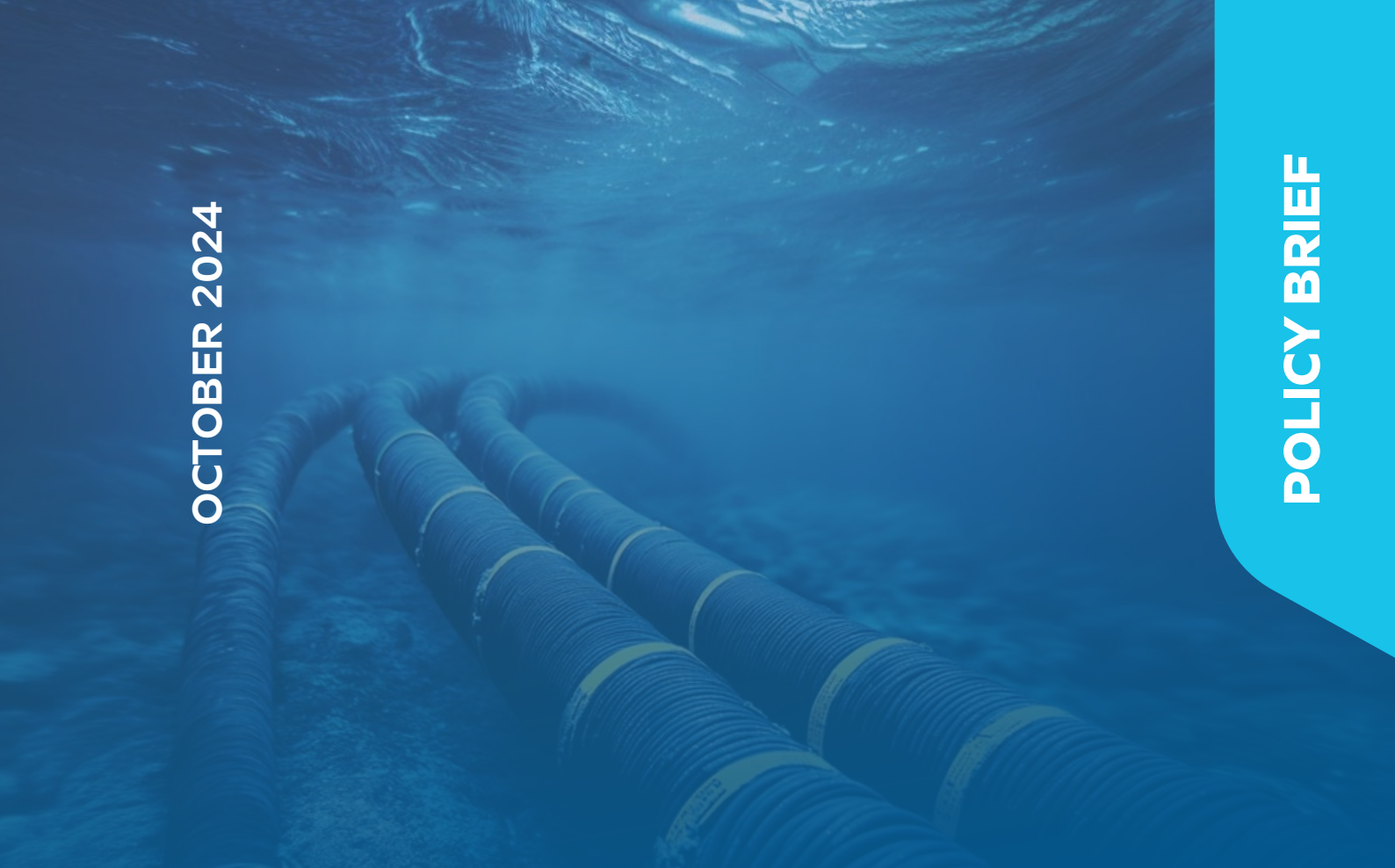

OCTOBER 2024

POLICY BRIEF

SUBSEA DATA CABLES SECURITY:

A Shared Concern for Global North and South

ALBERTO TAGLIAPIETRA & MOHAMMED SOLIMAN

10 YEARS POLICY CENTER FOR THE NEW SOUTH

G | M | F
IDEAS LEADERSHIP HOPE

PB - 55/24

POLICY CENTER FOR THE NEW SOUTH

10 YEARS

G | M | F

IDEAS LEADERSHIP HOPE

Subsea data cables are essential to the functioning of today's globally and digitally connected economies and societies. The world's emails, bank transfers, WhatsApp messages, and social media posts travel through undersea cables. Dependence on this infrastructure continues to deepen, leading states and regional organizations to recognize the need to provide adequate protection to an infrastructure that is fragile and vulnerable to unintentional (and intentional) disruption.

ALBERTO TAGLIAPIETRA & MOHAMMED SOLIMAN

RISING SECURITY CONCERNS

About 97% of global data runs through a few hundred undersea cables. These cables are vital to the global economy, spanning over 1.4 million kilometers, and connecting nearly all the world's countries. While most incidents involving disruption to undersea cables are unintentional, concern is rising about intentional actions amid increasing great power competition.

In 2023, at the Vilnius Summit, NATO launched the Maritime Centre for Security of Critical Underwater Infrastructure within NATO's Allied Maritime Command (MARCOM), aiming to better coordinate and protect this infrastructure. Similarly, the Quadrilateral Security Dialogue (QUAD), during its 2023 summit in Hiroshima, established a framework for cooperation on the protection of cables in the Indo-Pacific and also the G7, issuing a communique on the importance of collaborating more on undersea cable security. More recently, after experiencing massive internet outrages due to damage to subsea cables, Nigeria has been vocal within the International Telecommunications Union, the UN Agency for issues concerning information and communication technologies, asking for a new regional and global framework to be established to protect subsea cables better. Furthermore, during the 79th UN General Assembly, which took place in New York on September 22-23, 2024, the U.S. proposed a Joint Statement that would lay out principles to underpin the security, reliability, sustainability, and resilience of undersea cables in a globally digitalized world.

THE BACKBONE OF THE INTERNET

We are used to thinking about the internet as an intangible thing, yet its functioning is based on a huge network of data centers connected by thousands of kilometers of cables that sit at the bottom of the ocean. This physical infrastructure is the essential backbone that guarantees the functioning of the internet, and all the many activities based on it. Currently, there are more than 600 subsea cables in the world. The reason for such a large number lies in the resilience of a differentiated and distributed network, instead of localized and, consequently, more isolated and vulnerable, networks. Having multiple cables and different routes to connect the same dots is fundamental to increasing system reliability and avoiding bottleneck situations that can endanger the entire system. Yet, it also means that the infrastructure to safeguard the network is enormous in extension and growing every year. For this reason, it is essential to increase international cooperation to protect this infrastructure, as the current regime regulating this field does not do enough to mobilize efforts to create solid international protection.

When undersea cables are cut or damaged, the laws determining who is responsible vary depending on where the cables are laid. Coastal states have sovereign rights in their territorial seas and can exercise their rights to repair and maintain undersea cables in their exclusive economic zones. However, for cables that are damaged or sabotaged in international waters, there is currently no effective regime to hold the perpetrator of the damage responsible. Suppose cables are willfully or accidentally damaged by a ship or person in international waters. In that case, the jurisdiction to determine the measures against the perpetrator falls to the state under whose flag the ship operates, or that of the person's citizenship. The lack of a clear framework creates a strong need for international actors to take undersea cable security more seriously and establish internationally recognized protocols as part of a formalized protection plan that would act as a deterrent against sabotage of undersea cables, and prioritizes the security of digital communications.

A FRAGILE INFRASTRUCTURE

Undersea data cables represent an ideal target for disruptive actions, but as of today, there are no records of deliberate attacks against this infrastructure. Involuntary human activity is still the main reason for disruption. For example, in 2008, a cargo ship's anchor cut through the cables running between Italy and Egypt, causing disruption to millions of people and affecting 70% of internet and telephone traffic between Europe and Africa.

Similarly, natural events can cause damage to undersea data cables. For example, in late March 2024, four of the main cables serving West Africa were damaged by seismic activity, causing major issues in Ghana, Ivory Coast, Nigeria, Liberia, and Benin. Yet, there are also cases where the line between unintentional and intentional damage is thin. For example, in 2022, at least three cables connecting Marseille to Lyon, Milan, and Barcelona were cut off the French coast and, just a few days later, a cable connecting Scotland to the island of Shetland was also cut, causing disruption to mobile networks and impeding bank and ATM activities on the island for several days. While these accidents seemed unintentional, experts have expressed doubts about their nature and noted the presence of a Russian research vessel, the Boris Petrov, in the vicinity of these accidents, raising doubts about their cause.

The current situation in the Red Sea has also contributed to bringing the discussion about subsea cable security back into the international debate, particularly after a vessel struck by Houthi rockets dragged its anchor across three undersea data cables, disrupting part of the data traffic between Asia and Europe. What happened in the Red Sea is important because the Houthis have not only, intentionally or unintentionally, successfully carried out an attack on a critical infrastructure, but they have established a precedent, potentially inspiring other non-state actors to target these sensitive nodes.

The fragility of subsea data cables, coupled with the ease with which an attack can be disguised as an accident, and the potential heavy impact on the targeted country, make this infrastructure a great target for 'grey-zone' attacks, activities aimed at causing damage while remaining below the threshold of a full-scale response, by taking advantage of ambiguity and difficulty in attribution. This situation is tough to counter, as the infrastructure is fragile, relatively easy to disrupt, and difficult to repair. The issue is truly global and, to be addressed, will require strong cooperation between the Global North and Global South across the Mediterranean, the Atlantic, and the Indo-Pacific.

Furthermore, in addition to the risk of physical damage, there is also a security concern related to the possibility that certain actors could tap into the data running through subsea digital cables, thus intercepting data traffic. While this sort of operation would be difficult to carry out at sea, as it would require very sophisticated equipment and skills, it could be perpetrated at a landing station or by targeting the management systems used to operate the cables with a cyberattack. Such an attack happened in 2022 in Hawaii, when a hacking group was able to breach a private company's servers that manage an oceanic undersea cable that connects Hawaii and the Pacific region. While authorities were able to block the attack, this example showed that vulnerabilities exist, and it is crucial to stay vigilant.

Finally, the supply chain level might also constitute a potential risk. Cable building companies could potentially insert backdoors or install surveillance equipment before the cable is deployed. Notwithstanding the absence of such episodes in the past, attention is focusing increasingly on suppliers and vendors of undersea cables, signaling increasing

attention on the reliability and security of this infrastructure, particularly in times of rising geopolitical competition.

THE NEED FOR FURTHER NORTH-SOUTH COOPERATION

The current vulnerabilities of undersea cables, combined with the absence of international protection laws, put both developed and developing countries at risk. It is essential to increase collaboration to ensure the safeguarding of undersea cables, which can serve as a steppingstone for twenty-first century North-South economic and security cooperation.

While the United Nations Convention on the Law of the Sea (UNCLOS) offers a partial framework for protecting undersea cables in international waters, it focuses primarily on criminalizing negligent or intentional damage by vessels or individuals under a state's jurisdiction. However, UNCLOS lacks explicit provisions on the deliberate actions of state and non-state actors, underscoring a significant gap in legal protection. This legal blind spot necessitates greater reliance on developed nations. By leveraging their technological expertise and resources, developed nations should deploy advanced monitoring and protection systems for undersea cables. This focus is critical because developing nations, strategically positioned along key routes, house critical segments of this critical infrastructure. Developed nations can incentivize direct investments and technological localization in developing nations by enhancing security measures for undersea cables. Securing these cables near developing nations' shores mitigates the risks of global disruption caused by intentional or unintentional damage.

A cooperative North-South approach actively promotes best-practice sharing, joint investments in resilient infrastructure, and coordinated strategies for incident response. North-South cooperation can establish a global protection framework that addresses existing gaps in international regulations and strengthens collective response mechanisms. The Quad Partnership for Cable Connectivity and Resilience exemplifies this—it demonstrates how international cooperation can bolster submarine cable security in strategically important regions. International organizations such as the International Cable Protection Committee (ICPC) play a pivotal role in this collaborative North-South effort by facilitating dialogue and cooperation among governments, private-sector stakeholders, and international bodies, to harmonize protection standards and response protocols across regions, ensuring consistent and effective global efforts to safeguard undersea cables. This cooperation is in line with the principles of fair growth and mutual security, acknowledging that in an interconnected world, the vulnerabilities of one region can have widespread impacts.

The Joint Statement presented at the 79th annual United Nation General Assembly is a first step toward a global approach to the management and enhancement of the undersea data cables infrastructure. By covering elements related to construction, operation, surveillance, maintenance, and repair, and addressing the issues presented by landing stations, software, and the terrestrial parts of the infrastructure, the statement took a much-needed 360-degree approach. Covering all aspects of this infrastructure, from the supply chain to its deployment and how it is managed, and calling for broader cooperation between all actors involved in these several aspects, is the right direction to consolidate and make the infrastructure more secure. Yet, more needs to be done to bring as many states as possible on board, as only a few have endorsed the statement for the moment.

CONCLUSION

Subsea data cables are of vital importance to our societies. Mitigating the risk of intentional and unintentional disruption is a key element on which Global North and Global South stakeholders must increase their collaboration. To do so, it is essential to promote an international dialogue focused on cooperation and fair governance of submarine cable infrastructure. North and South should also join forces to increase monitoring capacities, reduce repairability time, and strengthen expertise and information sharing. Furthermore, it is crucial to address the uneven spread of the cable infrastructure across the globe, as its concentration in the Global North, and its scarcer presence in the Global South, lead to reduced resilience in case of damage to the infrastructure. To accomplish this objective, involving the private sector in the dialogue will also be crucial, as it is a fundamental player in this field. Seeking a cooperative approach is the best way forward, as this will help promote digital inclusion and enhance global connectivity, and will unlock the full potential of a more resilient and distributed infrastructure that will benefit both Global North and Global South.

ABOUT THE AUTHORS

ALBERTO TAGLIAPIETRA

Alberto Tagliapietra is Senior Program Coordinator at the Mediterranean Policy Program of the German Marshall Fund of the United States (GMF) in Brussels. His research interests focus on EU policies, migration, and the intersection between technology and migration. Alberto joined GMF in 2019. He holds a BA in international relations and an MSc in European and international studies from the University of Trento.

MOHAMMED SOLIMAN

Mohammed Soliman is the director of the Strategic Technologies and Cyber Security Program at the Middle East Institute, where he leads a global team of scholars to explore the policy challenges associated with the intersection of technology, geopolitics, and business in the Middle East and emerging markets more broadly. Mr. Soliman also serves as a visiting fellow with the National Security Program at Third Way.

ABOUT THE POLICY CENTER FOR THE NEW SOUTH

The Policy Center for the New South (PCNS) is a Moroccan think tank aiming to contribute to the improvement of economic and social public policies that challenge Morocco and the rest of Africa as integral parts of the global South.

The PCNS pleads for an open, accountable and enterprising "new South" that defines its own narratives and mental maps around the Mediterranean and South Atlantic basins, as part of a forward-looking relationship with the rest of the world. Through its analytical endeavours, the think tank aims to support the development of public policies in Africa and to give the floor to experts from the South. This stance is focused on dialogue and partnership, and aims to cultivate African expertise and excellence needed for the accurate analysis of African and global challenges and the suggestion of appropriate solutions. Read more

Policy Center for the New South

Rabat Campus of Mohammed VI Polytechnic University,
Rocade Rabat Salé - 11103
Email : contact@policycenter.ma
Phone : +212 (0) 537 54 04 04
Fax : +212 (0) 537 71 31 54

www.policycenter.ma

10 YEARS POLICY CENTER FOR THE NEW SOUTH

RePEc