ATLANTIC CENTRE

POLICY BRIEF ISSUE 13 | JULY | 2022

Protecting subsea data cables in Europe and the Atlantic – Challenges of a new era

Christian Bueger[1], Rita Costa[2], Tobias Liebetrau[3], Licínia Simão[4], Timothy Walker[5],

This Policy Brief is the result of the two-day workshop on "Maritime Infrastructures: Protecting subsea data cables in Europe and the Atlantic", held in Lisbon on the 29th and 30th of June 2022, on the sidelines of the United Nations Ocean Conference, in a partnership between the Atlantic Centre, SafeSeas, the University of Copenhagen, and the Institute for Security Studies in Pretoria. The workshop, which brought together academics and stakeholders from the industry, European institutions, and governments was held under Chatham House rules. While this does not allow us to name comments, we are grateful to all participants for their contributions to increase awareness of the importance of subsea data cable infrastructure, improving the understanding of the critical challenges and opportunities linked to the security of maritime infrastructure, and to facilitate a discussion on enhancing subsea data cable resilience in line with the goals of protecting marine ecosystems and biodiversity.

The workshop was supported by a Danish Agency for Higher Education and Science grant and funding from the Portuguese Ministry of National Defence.

[1] Professor of International Relations at the Department of Political Science, University of Copenhagen, honorary professor of the University of Seychelles, a research fellow at the University of Stellenbosch and one of the directors of the SafeSeas network (www.safeseas.net).
[2] Collaborator, Atlantic Centre.
[3] Researcher, University of Copenhagen.
[4] Professor in International Relations at the School of Economics and researcher at the Centre for Social Studies, University of Coimbra. Advisor to the Portuguese Minister of National Defence and Coordinator of the Atlantic Centre.
[5] Maritime Project Leader and Senior Researcher at ISS Pretoria.

INTRODUCTION

The subsea data cable network is essential to everyday lives and the functioning of states and their economy. The cable network carries around 99% of the global communications, and trillions of dollars of financial transactions daily. As such, today's globally and digitally connected societies are reliant on cables, and increasingly so as cable networks continue to expand in the face of the lack of other viable replacements.

Societies' dependence on these largely invisible infrastructures leads to increasing awareness – by national governments, international organisations, such as the European Union (EU) and the North Atlantic Treaty Organization (NATO), and the United Nations – that subsea data cable networks are core critical infrastructures.

A stark recognition has accompanied this newfound awareness of the importance of subsea cables. Dependence on these infrastructures is growing exponentially, yet their security has been largely overlooked and left in the hands of the private sector. The recognition that the protection of subsea data cables is a matter of national and regional security has been changing this outlook and furthering governmental efforts to increase their protection. The rise of new threats, such as hybrid warfare and cyberattacks, along with the current geopolitical environment, add to the sense of urgency in securing and increasing the resilience of these critical infrastructures.

In this policy brief report, we argue that these developments represent the beginning of a new era for the subsea data cable system. This brief aims to contribute to the discussion on ensuring the security of subsea data cables in complementarity with other maritime and cyber governance issues. The policy brief is structured in two parts. The first part sets forward an overview of the strategic importance of cables, how the cable network works, and lays out the critical vulnerabilities of cable infrastructure and the consequences for states. The

second part brings together the main obstacles and proposed options for the effective governance of cable infrastructure (as discussed at the workshop) to launch the discussion on the challenges associated with the new era.

The strategic importance of subsea data cables

With Russia's war in Ukraine, the increasing US-China competition and technological decoupling, as well as the EU's search for digital sovereignty, the strategic importance of critical infrastructure protection, technological dependencies and supply chain risks are paramount. Contemporary geopolitical and geoeconomic struggles often now include significant efforts to achieve digital superiority.

Subsea data cable infrastructure is increasingly recognised as a critical part of the digital era. A significant cable outage would disrupt most aspects of the functioning of our digital societies and daily life. A partial shutdown of digital data transmission would lead to significant disturbances in the health, defence, diplomatic, and economic sectors and other activities essential for national welfare and security.

With the arrival of the 5-6G network, the Internet of Things, artificial intelligence and increasing cloud storage, the demand for data transfer will only increase. Everything from public services over industrial production to citizens' everyday lives will become even more dependent on the smooth functioning of subsea data cables, elevating the strategic importance of the cable infrastructure, especially considering the limitations of satellite technology in supplementing big data transfers.

Vulnerabilities to the subsea cable network

Over 400 undersea cables spanning at least 1.3 million kilometres are currently in service. The distribution of these cables is uneven across the world. For instance,

the North Atlantic hosts one of the world's highest densities of subsea cables. This is important as regions, states or territories with more cable redundancies (including land-based cable connections) are less likely to experience connectivity loss due to cable ruptures. The small island developing states tend to be more vulnerable, which was recently demonstrated by the effects of the 2022 Hunga Tonga–Hunga Ha'apai eruption and tsunami. The Global South is generally more susceptible to interruptions due to a much lower number of redundancies and density of cables and the impossibility of land cable alternatives compared to most states in the Global North.

Furthermore, other elements impact a region, state or territory's level of vulnerability to cable faults, such as landing site diversity and availability of repair capacities. In the first case, a concentration of landing sites near each other enhances the likelihood of simultaneous disruptions. Greater availability and proximity of repair capacities accelerate the repair of faults to a degree, lessening their consequences, even in the event of multiple simultaneous failures.

There are around 100 cable faults per year, on average. In general terms, the causes of these faults can be divided into three categories: external, natural and human-based.

External incidents that can threaten the functioning of the cable system could be, for instance, electrical blackouts or outages of land-based internet infrastructures. Economic factors can also fit into this category, as disruption in global value chains on the production or transport of repair parts, bankruptcy of the operators or maintenance companies, and potential shortfall of workers could all affect the cable network.

Naturally caused cable faults could occur due to seismic activity, extreme weather events, and black swan events. These natural events might simultaneously damage a significant number of cables, causing major disruptions even in states with several redundancies. Climate change amplifies these threats in terms of

impact and likelihood if coastal areas and low-lying inland areas become increasingly inundated and eroded.

Human-based faults can either be accidental or intentional. Accidents are by far the leading cause of cable ruptures, namely fishing and anchoring, among others. In contrast, deliberate attacks tend to be rare. However, the current geopolitical environment of heightened geopolitical competition, along with the evolution and broader accessibility of technology, has significantly raised levels of concern over intentional attacks.

Attacks can aim to physically destroy the cable infrastructure or be carried out with the intent to obtain information the cable system carries. The physical destruction of cables could be carried out, for instance, through the use of weaponised civilian vessels such as fishing vessels, Maritime Improvised Explosive Devices (MIED) or military-grade naval mines, and manned or unmanned underwater vehicles. Data theft could be performed through taping cables or hacking. Additionally, cyberattacks are also a growing concern due to the cable networks' dependence on remote network systems and the substantial capabilities of hostile state and non-state groups.

Generally, attacks are more likely in shallow waters or against landing stations due to the inherent difficulties of reaching cables laid in the deep seas and the approximate location of cables in these areas being available as open-source information. This exposes a dilemma on cable protection, as gatekeeping information on their location protects them from intentional attacks while it enables the likelihood of accidental damage.

Key challenges for improving cable resilience in Europe and the Atlantic

Improving cable resilience in the new era is confronted with various challenges, many of which require innovative political thinking and initiative. We set out seven of the key challenges and discuss how they might be addressed.

Complexity

As a regulatory and political issue, cable governance and protection intersect with different policy fields, each with dissimilar legislations, agencies and authorities involved. This includes media and telecommunication policy, maritime security policy, cyber security policy and critical infrastructure protection. At a state level, this implies that various legislative and executive committees are involved, as are agencies, ranging from telecommunications regulators, maritime authorities, navies, coastguards, marine police, cyber security agencies and others involved in critical infrastructure protection. Moreover, cables cross through jurisdictional zones, land territory, where typically the police or technical regulators are in charge, territorial waters, where coastguards and marine police have a mandate, and international waters, where navies are the responsible actors. Some countries manage to harmonise these different policy areas, regulations and actors better than others. Yet, effective communication between national authorities and industry is an intricate challenge.

These harmonisation and communication challenges accelerate if one takes a regional perspective. The number of relevant political processes, regulations and agencies in the European Union substantially increases. Some aspects of the regulation lie within EU-wide jurisdiction, and various agencies are mandated to support member states in maritime or cyber security fields.

Both within states and the EU, the complexity must be addressed by improving mutual understanding through information sharing on regulations, best practices, incidents and suspicious behaviour, but also via dedicated coordination instruments. Dedicated coordination bodies are required to move this forward.

In other regions, such as the North-Atlantic or South-Atlantic, existing coordination between states, their agencies, and the industry is weaker. Here solutions must be identified where cable protection can be coordinated, either within existing institutions or in informal formats.

Taking such steps is even more critical given that one of the implications of the new era is that more actors are likely to get involved. Due to the new awareness, this might imply that policymakers ask other agencies that do not play a role to date to contribute to cable resilience, and hence complexity further increases.

Addressing the knowledge gaps

One of the implications of the new era is the novel degree of attention to the vulnerabilities of the cable system. Public media increasingly discuss the issue, and parliaments have started to engage, as have security officials. There remains, however, a considerable lack of knowledge on how the cable system functions, what national, regional and international rules govern it, how the cable industry is organised, or what the actual vulnerabilities are. A range of myths circulate such as the legend that shark attacks are a vital threat to the cables, and doomsday scenarios are floated suggesting that the risk and impact associated with the Tonga cable cut also apply to European states or that an adversary could cut off European states from the internet entirely. There is hence a need not only to confront such myths and misleading scenarios, but also to increase the level of publicly trusted and available knowledge and information sources.

This also implies taking steps to improve the education and training of those that have or will have, a role to play in protecting cables. Basic knowledge of the cable system should be integrated into the education and training of agencies, particularly coast guards and navies.

Using existing capacities

In the past decade, nation states and the European Union have developed substantial capacities for maritime surveillance and information sharing. These capacities were primarily developed to enhance marine safety and shipping, monitor fisheries, or counter blue crimes, such as people smuggling or piracy. Such capacities could also be employed to improve cable resilience.

Maritime Domain Awareness platforms, such as the one operated by the European Maritime Safety Agency (EMSA), can draw on different surveillance technologies, including satellite images or drones that can be used to monitor marine activities in cable locations and detect suspicious behaviour. Information sharing platforms, such as the Common Information Sharing Environment of the EU, could also be used to exchange data on cable-related incidents or suspicious behaviour. This could significantly enhance monitoring, surveillance, data sharing, and inter-agency collaboration.

A clear-cut assessment is needed of which existing capabilities could be used to monitor cables and what practical hindrances persist in employing them in such a way. This also implies identifying gaps.

Subsea blindness

While many capabilities and technologies have been developed in Europe and elsewhere to monitor and understand behaviour on the maritime surface, the same cannot be said for the subsea. The subsea and seabed remain one of the planet's least understood and researched spaces. Given the ocean floor's vastness and cable systems' length, monitoring cables undersea will be challenging. This calls for advancing new undersea surveillance technologies, for instance, through automated subsea vessels. Several technologies will be dual use and will likely play a role in submarine warfare too.

How to use smart cable data

One of the technologies already available are sensors built into the cable systems. Cables are increasingly becoming smart and capable of collecting data on their environment. Current cable systems are equipped with Distributed Acoustic Sensing (DAS) systems. DAS is primarily used to detect the location of cable faults and is capable of recording movements close to the cable. There are other technologies in an advanced stage of development. Polarisation technologies and new measurements using laser light provide other sensors and can potentially also upgrade older telecommunications cables.

The benefits from such sensing technologies go beyond cable protection. Data can provide insights for modelling ocean waves or detecting seaquakes and might hence be helpful in disaster prevention. Whether and how smart cables can play a role in submarine warfare and subsea vessel detection has not yet been fully elaborated, but this is at least a plausible future scenario.

The smart cable evolution raises a range of questions. Firstly, if sensors provide an essential layer for cable resilience, how can such technology be made compulsory, and how can innovation be enabled? Second, what provisions are required to regulate the use and availability of sensor data for private, governmental and scientific use? Regulatory measures are likely needed to address these issues.

Cable diplomacy and capacity building

Cable infrastructures are transnational. A purely national or regional perspective is not enough. Cable systems connect and disconnect countries and regions across the globe. They also establish new dependencies and vulnerabilities. Cable resilience hence belongs both on the diplomatic and development agenda.

Cables connect countries. In some cable routes, critical bottlenecks exist. For European connectivity, this is Egypt through which the connections to Asia are

routed. Placing the issue on the EU-Egyptian diplomatic dialogue is hence required.

Moreover, countries in the Global South, particularly the small island developing states, are exposed to several different challenges and will remain more vulnerable to outages and disruptions than countries in the Global North. Some countries depend on a single cable connection and are seen as feasible markets upon which to expend investment on additional cables. Given the importance of cables for developing digital economies and the lack of capacities in many countries, cable protection has to feature on the development agenda, and should be part of existing or planned capacity-building programmes. For instance, regarding the African Union (AU) and its member states, making digital connectivity a key initiative will arguably be essential for anchoring Africa's economic growth and development. Connectivity does feature in several flagship projects of the AU's Agenda 2063, but only pertaining to transport via rail and air connections.

Cables and marine conservation

One issue that requires further exploration is how cable resilience measures and marine conservation goals can support each other. Marine protected areas that limit marine activities in particular spaces can be a tool to protect marine biodiversity and cables simultaneously. Yet, different marine users often interpret each other as rivals over ocean space and do not necessarily have a culture of cooperation. Current research points out that disruptions to the marine environment due to cable laying and maintenance are minor; hence, conservation and cable protection can mutually reinforce each other. This implies well-executed marine spatial planning processes, in which the expanding cable industry should be a significant stakeholder. It also requires better consideration of how limited maritime security capacities are most effectively used to enforce the rules installed in such planning processes.

Further Reading

Bueger, Christian and Tobias Liebetrau. 2021. Governing hidden infrastructure: The security politics of the global submarine data cable network, *Contemporary Security Policy*, 42(3), 391-413.

Bueger, Christian, Tobias Liebetrau and Jonas Franken. 2022. *Threats to undersea communications cables and infrastructure – consequences for the EU*, In-Depth Analysis for the European Parliament commissioned by the Sub-Committee on Security and Defense, 1.6.2022, https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557

Burnett, Douglas R., and Lionel Carter. 2017. "International Submarine Cables and Biodiversity of Areas Beyond National Jurisdiction." *Brill Research Perspectives in the Law of the Sea* 1 (2): 1–72.

Medeiros, Sabrina Evangelista and Danielle Jacon Pinto Ayres. 2022. Cabos submarinos e segurança cibernética no Atlântico. *Atlantic Centre Policy Brief* n. 11, March. https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_11.pdf