Minds and Machines (2024) 34:31
https://doi.org/10.1007/s11023-024-09683-z

Submarine Cables and the Risks to Digital Sovereignty

Abra Ganz[1] · Martina Camellini[2] · Emmie Hine[1,2,3] · Claudio Novelli[1,2] · Huw Roberts[4] · Luciano Floridi[1,2]

Received: 14 January 2024 / Accepted: 10 June 2024 / Published online: 8 July 2024

Abstract

The international network of submarine cables plays a crucial role in facilitating global telecommunications connectivity, carrying over 99% of all internet traffic. However, submarine cables challenge digital sovereignty due to their ownership structure, cross-jurisdictional nature, and vulnerabilities to malicious actors. In this article, we assess these challenges, current policy initiatives designed to mitigate them, and the limitations of these initiatives. The nature of submarine cables curtails a state's ability to regulate the infrastructure on which it relies, reduces its data security, and threatens its ability to provide telecommunication services. States currently address these challenges through regulatory controls over submarine cables and associated companies, investing in the development of additional cable infrastructure, and implementing physical protection measures for the cables themselves. Despite these efforts, the effectiveness of current mechanisms is hindered by significant obstacles arising from technical limitations and a lack of international coordination on regulation. We conclude by noting how these obstacles lead to gaps in states' policies and point towards how they could be improved to create a proactive approach to submarine cable governance that defends states' digital sovereignty.

Keywords Digital sovereignty · Internet · Submarine cables · Surveillance · Critical infrastructure

✉ Abra Ganz
abra.ganz@yale.edu

[1] Digital Ethics Center, Yale University, 85 Trumbull St., New Haven, CT 06511, USA

[2] Department of Legal Studies, University of Bologna, Via Zamboni 27/29, 40126 Bologna, Italy

[3] Centre for IT & IP Law, KU Leuven, Sint-Michielsstraat 6, 3000 Leuven, Belgium

[4] Oxford Internet Institute, University of Oxford, 1 St Giles', Oxford OX1 3JS, UK

1 Introduction

Transmitting data to communicate internationally depends on a global network of physical cables lying under the sea, known as the *submarine cables infrastructure* (SCI); see Fig. 1. With a total length of 1.4 million kilometres, over 99% of all internet traffic passes through the SCI (Mauldin, 2023). If some of these cables were cut, global communications would be severely slowed. If all of them were cut, the global internet would cease to exist. For instance, if the 40 cables connecting the US to the rest of the world were severed, it is estimated that only 7% of US internet traffic could be carried by alternate satellite infrastructure (Liu et al., 2020).

Existing research on the SCI has largely focused on three specific areas of study: (1) security and military issues, i.e. how to protect the SCI from hybrid warfare and terrorism; (2) technical and operational issues, i.e. what are the daily risks, damages, and the necessary maintenance for the SCI's operation caused by accidental damage and non-human hazards; and (3) international regulation issues, i.e. examining current international regulations governing the SCI and questioning whether they require improvement (Bueger & Liebetrau, 2021). Since the SCI plays a critical role in determining internet access and is vital to the development and proliferation of emerging technologies such as 6G, IoT, and cloud computing, its importance has grown considerably in recent years, solidifying its status as a strategic asset.

However, thus far there has been no comprehensive analysis of individual countries' approaches to SCI governance for routine application—the everyday provision of secure telecommunications to a populace at large. Nevertheless, the significance of submarine cables for global internet connectivity, coupled with concerns over

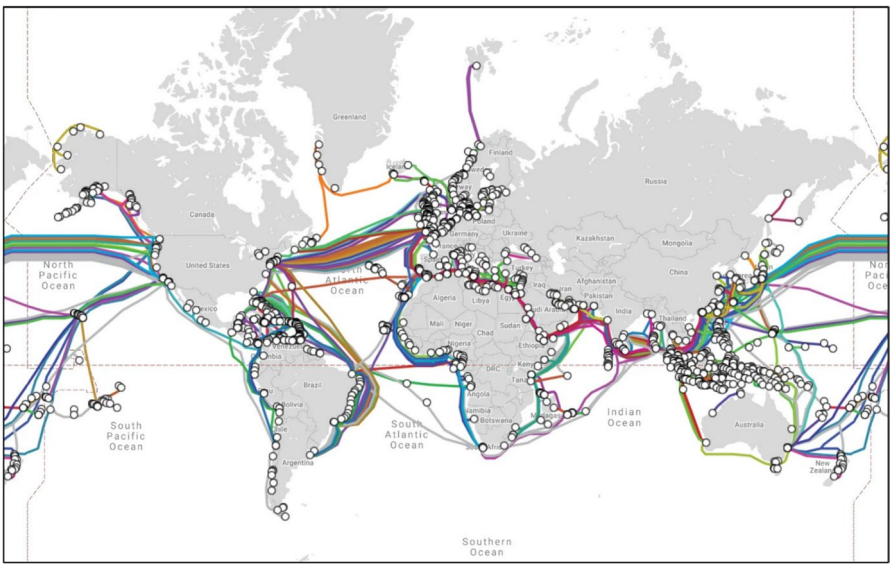

Fig. 1 A map of submarine cables. Source: telegeography.com under license CC BY-SA 4.0

cyber security and geopolitical tensions, merits an examination from the perspective of nations seeking to assert greater control and autonomy over their digital resources and data flows. Hence, in this article, we address this research gap by analysing the role that the SCI plays in states' pursuit of digital sovereignty, understood as "the control of data, software (e.g. AI), standards and protocols (e.g. 5G, domain names), processes (e.g. cloud computing), hardware (e.g. mobile phones), services (e.g. social media, e-commerce), and infrastructures (e.g. cables, satellites, smart cities)" (Floridi, 2020). In the context of submarine cables, digital sovereignty encompasses the authority of nations to dictate the routes and locations where cables are laid within their territories, establish standards for the cables and the data transmitted through them, and ensure robust protection to sustain internet provision and safeguard the privacy of transmitted data. We believe that the SCI has been left out of conversations on digital sovereignty thus far because of its invisible nature as subsea infrastructure and in large part exactly due to states' lack of control over it. While it is a critical part of infrastructure, states have, for the most part, not engaged with it: most have not created domestic legislation nor joined international forums for discussion of its standards and protection. This has recently begun to change with the EU Commission publishing recommendations and opening a public consultation in February 2024 on how to protect the SCI (European Commission, 2024). We discuss not only how states assert their own digital sovereignty but also how they infringe upon the sovereignty of others, extending their influence as they extend the cable network. The infringement of digital sovereignty can be extended to other actors, such as technology companies, who can themselves assert control over the digital as (quasi-)sovereign actors (Tretter, 2022).

The article is structured as follows. Section 2 provides a brief background: an overview of the current international regulation and public and private stakeholders in the SCI. Section 3 explains the risks that submarine cables pose to countries' digital sovereignty in terms of their data, the provision of internet-based services, and countries' control over their technological infrastructure. Section 4 examines states' current strategies to increase their digital sovereignty concerning submarine cables. Section 5 details the limitations of the existing mechanisms and points towards how they could be improved. Section 6 concludes the article.

2 Background

The complexity of SCI governance arises from two main factors: the requirement for international cooperation from various state actors, who may act against each other for strategic gain, especially in potential conflict scenarios, and the significant ownership of the SCI by private entities, whose interests may be misaligned with states' interests, including the governments of the territory they are domiciled in (Bueger & Liebetrau, 2021). This makes governance of the SCI more complex than other cross-border infrastructures which suffer from the same types of competition, such as water or oil pipelines. Although submarine cables and pipelines have different polluting capabilities and routes, they are often grouped together in international law, since they traverse all ocean categories, require similar preparation for

installation, and suffer analogous challenges of international cooperation. In other cases, there is usually more functional international governance and either no owner or a singular owner of the commodity being transferred, rather than, in the case of data, a multiplicity of owners and stakeholders. Thus, when considering a country's digital sovereignty over submarine cables, one must consider both international relations (country-to-country) and interactions between governments and private companies (country-to-company). In this section, we briefly review the roles of public and private stakeholders in the SCI and the relevant legislation.

2.1 Country-to-Country: Current Regulation

The United Nations Convention on the Law of the Sea (UNCLOS) is the predominant international treaty governing the rights of installation and protection of submarine cables. It came into force in 1994 and, at the time of writing, has 169 parties (168 individual states and the European Union), which does not include the United States ('Chronological Lists of Ratifications of Accessions and Successions to the UNCLOS and the Related Agreements' 2023). However, the US recognises UNCLOS as part of customary international maritime law (US Department of Commerce, 2023). UNCLOS ratifies a country's ability to formulate its own regulation on submarine cables near its shore and asserts the right of any country to establish submarine cables beyond these boundaries.

UNCLOS has five main articles which govern the installation and regulation of submarine cables in the four different UN classifications of maritime areas. Articles 21(c), 58, and 79 cover territorial seas, exclusive economic zones, and the continental shelf, respectively, and articles 87(c) and 112 cover the high seas. In the high seas, all states, whether coastal or landlocked, are allowed to lay submarine cables (subject to a few conditions, such as a lack of interference with pre-existing cables). All actors are allowed to lay cables in the continental shelf, subject to agreement on the route with the coastal country. In exclusive economic zones, which extend up to 200 nautical miles from the coastline, actors are subject to route agreements and local regulations. The territorial sea is the only area where each state has a right to exercise its sovereign authority and can set its own regulatory regime for when to allow actors to lay new submarine cables. According to UNCLOS, a country can claim a territorial sea of up to 12 nautical miles from its coastline or until the median point between the country and another country, whichever is lesser. The result is that, within territorial seas and the exclusive economic zone, the territory is under the jurisdiction of the governing state. Beyond this, only ships are under a jurisdiction, namely that of their flag. UNCLOS requires that ratifying states introduce legislation for their flag-bearers against intentional or negligent damage (articles 113, 114, and 115). Nevertheless, there is an ongoing debate about how to interpret these articles in light of case law precedent. Recently, it has been argued that, in some cases, cable damage could be attributable to countries even outside of their jurisdiction, in which case they would be liable for the value of submarine cable repair and any losses stemming from damage to a submarine cable (Guilfoyle et al., 2022).

This situation makes it challenging for any country to ensure cable safety independently (Frazier, 2023). Further, given the borderless nature of the internet and the high seas, submarine cables sit between two areas of limited regulation and ambiguous governance responsibilities. This leads to a regulation gap; states allow private ownership of critical international infrastructure while failing to introduce legislation to protect this infrastructure—few countries have any legislation that protects the SCI and UNCLOS offers little security (Aldrich & Karatzogianni, 2020).

Although international regulatory frameworks are insufficient to ensure cable protection, there is an international forum, the International Cable Protection Committee (ICPC), to discuss technical, legal and environmental information relevant to the SCI. Its membership primarily consists of commercial companies that own, operate, or have an interest in submarine telecommunications or power cables, covering most of the world's major cable system owners and operators. The membership also includes government organisations from ten different countries and a small number of research institutions ('Member List',2023). The ICPC can, however, make only recommendations; binding decisions are the purview of nation-states.

2.2 Country-to-Company: Public and Private Stakeholders

Governments are strategically interested in protecting and maintaining the SCI due to its societal, economic, public health, and safety implications (Liu et al., 2020). In particular, governments should prevent technical failures and address threats that can jeopardise critical infrastructure. As the internet is the backbone of many economic activities and telecommunications, monitoring foreign intrusions and various system vulnerabilities, stemming from natural and artificial hazards, is a critical factor that guides countries in shaping their digital strategy and reducing dependence on foreign technologies.

Although governments have a strategic interest in maintaining these cables, they lack any legal obligation, as we saw above, and the significant role of the private sector further complicates their ability to have any sort of sovereignty over the SCI. In the past, submarine cables were typically owned by telecom carriers, which had ties with governments and would form a consortium of interested parties. However, as of December 2020, 59% of submarine cables were owned entirely by actors in the private sector, see Fig. 2 (Sherman, 2021). This trend is expected to continue or even rise as private investments in submarine cables from companies such as Google, Meta, Huawei, and Amazon are increasing to meet their expanding bandwidth needs (Satariano et al., 2019). Also known as hyperscalers or "over-the-top" service providers, these companies can afford to fund submarine cables (such as Google's Curie and Durant cables) independently, thus gaining substantial control over a large proportion of the international communication network.

Hyperscalers' growing power over the telecommunications network and hence growing influence over states and other companies can be understood through the framework of weaponised interdependence (Gjesvik, 2023). Introduced by Farrell and Newman in 2019, it was originally defined as occurring where "states with political authority over the central nodes in the international networked structures

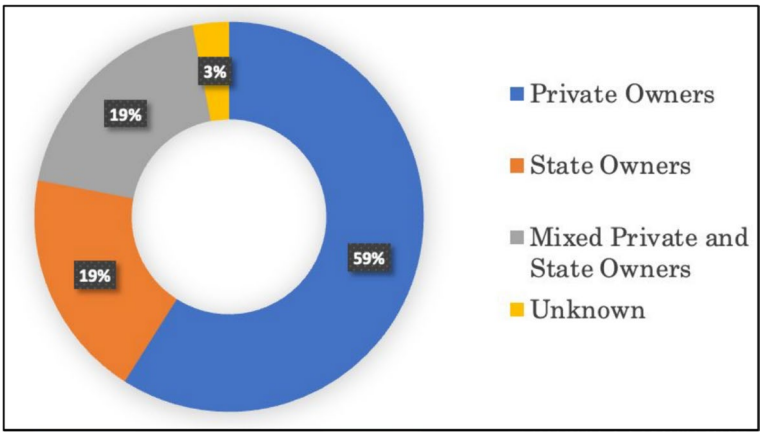

Fig. 2 The ownership of submarine cables. Source: Data from telegeography.com, visualised by author

through which money, goods, and information travel are uniquely positioned to impose costs on others" (Farrell & Newman, 2019). It has since been extended to cover companies as well. In the context of the SCI, the increasing ownership and provision of encryption services have made companies necessary middlemen in the global communications network and, consequently, arbiters of state power (Gjesvik, 2023).

Consequently, companies can influence SCI government policies. This could be through promising future funding for infrastructure projects or through their control over existing infrastructure. Promises of substantial benefits from new infrastructure significantly increases companies' lobbying power. For example, in 2021, Google promised Nigeria that its new Equiano cable would improve median download speeds by up to six times, reduce retail data prices by 21%, and create economic activity that would indirectly result in $10 billion added to Nigeria's GDP (O'Carroll, 2021). While it is unclear what influence this infrastructure investment had or will have on Nigeria's government policy, substantial economic incentives play a pivotal role, whether in SCI policy or policy more generally. Companies can also indirectly affect a country's digital sovereignty by using their control of a submarine cable to prioritise their choice of traffic through existing cables. For example, where telecom companies are focused on the end customer, hyperscalers want to prioritise keeping their services running and, as a result, give precedence to traffic between their own data centres. This would undermine the principle of net neutrality. As submarine cables typically traverse between two or more regulatory jurisdictions and since there is little regulatory consensus on net neutrality, it is unclear how countries would effectively regulate companies' prioritisation of traffic.

Influence, however, can go both ways. Countries can influence company behaviour through mechanisms, such as regulation and political pressure, and use companies to increase influence abroad. Although there has been a rise in the proportion of submarine cables owned by private companies, many of these companies are entirely or partially owned by a government, such as the Hengtong Group, owned by

China (Colombo et al., 2021), or Telecom Egypt (TE), 70% owned by Egypt (Werr, 2023). Further, even when not government-owned, companies can be influenced by a government either through direct regulation or soft power. For example, in 2020, HMN Tech, owned by Chinese company Huawei, was selected to manufacture and lay a new Singapore-to-France cable owned by a consortium of Chinese, American, and French companies. However, given the US government's apprehension regarding security risks associated with sensitive communications cables, particularly following concerns related to Chinese involvement, efforts were made to transition the contract to another company, SubCom. This campaign proved successful through a combination of incentives and diplomatic pressure on consortium members (Brock, 2023), combining digital sovereignty measures with digitally expansionist behaviour (Roberts et al., 2023).

The degree to which governments can use digital giants in the submarine cable market as soft-power leverage is debated due to the increasing independence of these hyperscalers. On the one hand, as countries grow dependent on these privately-owned cables, they also become influenced by the policies and attitudes of the cable owners' home countries. For instance, Carr discussed in various publications how the internet's multi-stakeholder model, involving diverse groups in its infrastructure, amplifies US foreign influence (Carr, 2015; Suganami et al., 2017). This occurs despite the US having a limited official role in the development of the internet's infrastructure. Carr's argument is exemplified by the fact that many key internet technologies and companies, such as Google and Amazon, give the US an indirect influence over global digital communications. On the other hand, the increasing globalisation of multinational corporations means that the countries in which they are domiciled have diminishing influence over them as they develop increasing power to pursue their own interests. In particular, Gjesvik notes that while the dominant hyperscalers are US based, this apparent centralisation of power must be considered in conjunction with the weakening authority of the US government domestically (Gjesvik, 2023).

3 Risks to Digital Sovereignty

It may appear that the main concern regarding the SCI is breakages hindering the provision of telecommunications. Yet it is also a serious risk to countries' digital sovereignty if the infrastructure that they rely on for that provision is owned and controlled either in the most part or in whole by external countries and companies. Further, if a country cannot protect the privacy of its own data, it can hardly be held to have sovereignty over that data—and the low rates of data encryption give rise to easy communication interception via wiretapping. Hence the complexities of country-to-company and country-to-country interactions challenge countries' digital sovereignty in three areas: the ability of a country to control its technological infrastructure, to control its data (data security), and to provide internet-reliant services.

3.1 Infrastructure Regulation

The transnational and marine nature of submarine cables threatens a country's ability to control its telecommunications infrastructure. This control is "the ability to influence something (e.g. its occurrence, creation, or destruction) and its dynamics (e.g. its behaviour, development, operations, interactions), including the ability to check and correct for any deviation from such influence" (Floridi, 2020). It includes the ability to set standards, establish regulatory frameworks, and allocate licensing agreements.

As the submarine cables on which a country relies are often owned by foreign companies and countries over which the reliant country has no jurisdiction, that country lacks formal means of control over any part of the SCI outside its territorial seas under current regulation (Carr, 2015). In some particularly acute cases, multiple countries claim jurisdiction over the same waters, meaning that the cables traversing them are subject to differing interpretations of which legislation applies to them. For example, Turkey contests the Aegean Sea (with Greece) and the Levantine Sea (with Greece and Cyrpus) which cables such as the MedNautilus and the BlueMed traverse (Bueger et al., 2022). Furthermore, many countries have no submarine cables travelling through their territorial seas or have no territorial seas at all, resulting in no jurisdiction over any part of the SCI and a reliance on contiguous coastal countries that have SCI landing points, see Fig. 1.

One can use comparisons with oil and gas pipelines to bring countries' reliance into focus. While each country can, to some extent, produce its own energy (just as many countries have their own data centres with cached versions of much of the internet), if a country decides to cut off a pipeline's supply, as was seen with Nord Stream 1 where Russia cut gas supplies to Europe by 88% and gas prices in Europe more than doubled (*BBC* News, 2022), this can have devastating effects on citizens' wellbeing and countries' economies. This analogy is imperfect: oil pipelines are unidirectional while submarine cables are bidirectional. Oil is a physical commodity transferred from one country to another while internet traffic travels both ways; if one country is disconnected, not only is it cut off from other countries' digital output, but other countries are also severed from its own. Still, it helps to illustrate the significance of the problem.

It is difficult to solve the problem of SCI control. Submarine cables have many indirect stakeholder states due to the decentralised nature of the internet, with any country that communicates with services based on a different landmass utilising the SCI. Attempting to bring every stakeholder, even only on a state level, into conversation and agreement on SCI standards, usage, and other issues, would require high coordination effort. The ICPC might be expected to take on much of this role. However, this is undermined by its lack of government membership and its inability to make binding decisions.

3.2 Data Security

The ability of a country to control its data, whether military or civilian, is at risk because of the vulnerability of submarine cables to wiretapping. Over 99% of all international internet traffic is sent via submarine cable. The remainder is

sent via satellite communication, which is highly vulnerable to interception as the data is openly transmitted via the air (Tedeschi et al., 2022). However, submarine cables have their own vulnerabilities. If one has access to a submarine cable, either at its landing points or anywhere along its length, all data passing through it can be gathered. Admittedly, much of it is encrypted; however, it is difficult to determine what percentage of internet traffic is encrypted since much of it is private. 80–95% of traffic through browsers such as Firefox and Google Chrome is encrypted, up from 55% in 2017 (Google, 2023; Let's Encrypt, 2023), likely reflecting broader trends in encryption levels. However, despite the levels of data encryption making upstream data collection much more appealing, there are still worries about espionage due to two factors: the potential for reading unencrypted data, such as metadata and most emails, and the potential for later decryption of encrypted data that is gathered now. This may be possible within the next two decades via new quantum computing techniques (Kramer, 2023).

The combination of the ability to access currently unencrypted data and the potential for decrypting currently encrypted data in the future raises significant concerns about the ease of accessing submarine cables and thereby the data they carry. Currently, all that is required to tap a submarine cable is access to the fibre-optic cables in its core. An early example of cable tapping occurred in 1970 when the US tapped an undersea cable between the Soviet fleet's Pacific base and its headquarters in Russia (Hoffman, 2010). The US continued to use this technique as recently as 2015, ensuring they could see any data passing through an AT&T-owned cable in the United States (Angwin et al., 2015). Some points are particularly at risk, such as the Suez Canal, since the networks that pass through the Suez Canal are still among the busiest in terms of telecommunications traffic, making it an attractive place for cable espionage (Aluf, 2023). The relative ease of tapping is due to the lack of security around submarine cables; there are 1.4 million kilometres of submarine cables, making protection methods such as patrols or greater physical protection cost-prohibitive.

These risks are exacerbated by countries trying to influence the SCI via various means to gain greater access to its traffic (Sherman, 2021). Countries might attempt to shape the SCI's topology to route more traffic through their country, thereby granting themselves landing-point access to cables and facilitating data gathering. For example, in the past the central locations of the UK and US in the SCI gave them 'unrivalled intelligence capabilities' (Gjesvik, 2023). Countries can also create closer ties with cable owners to take advantage of their cable access (Ghiasy, 2020) or develop closer relations with cable builders for the same reason (Sherman, 2021). All countries rely to some extent on foreign-owned submarine cables in foreign jurisdictions and international waters for data transport. This risk cannot be alleviated given the global nature of the internet. However, countries vary in the extent to which they allow foreign-owned companies to operate within their borders, which impacts their control over their own infrastructure.

3.3 Internet-Reliant Services

The ability to provide internet-reliant services is at risk from the vulnerability of submarine cables to physical damage. If a cable is damaged, traffic is slowed or cut off entirely. The social and economic effects can be significant: one estimate puts the direct value of the SCI to the US economy at $649 billion in 2019 (Goodman & Wayland, 2022). Further, if the subsea cables connecting one country to others are cut, it is not just the digitally isolated community that suffers; the impact also extends to other parts of the world that rely on constant communication with that community. Taiwan, for example, holds a leading position in the technology industry, particularly in microchip manufacturing, due to the prominence of TSMC. If the cables connecting the Taiwanese mainland to the global internet were cut and it needed to rely solely on satellite traffic, there would be significant consequences to the global chip supply chain. This is particularly relevant since US-China tensions have recently increased in the domain of computer chips, with the US introducing

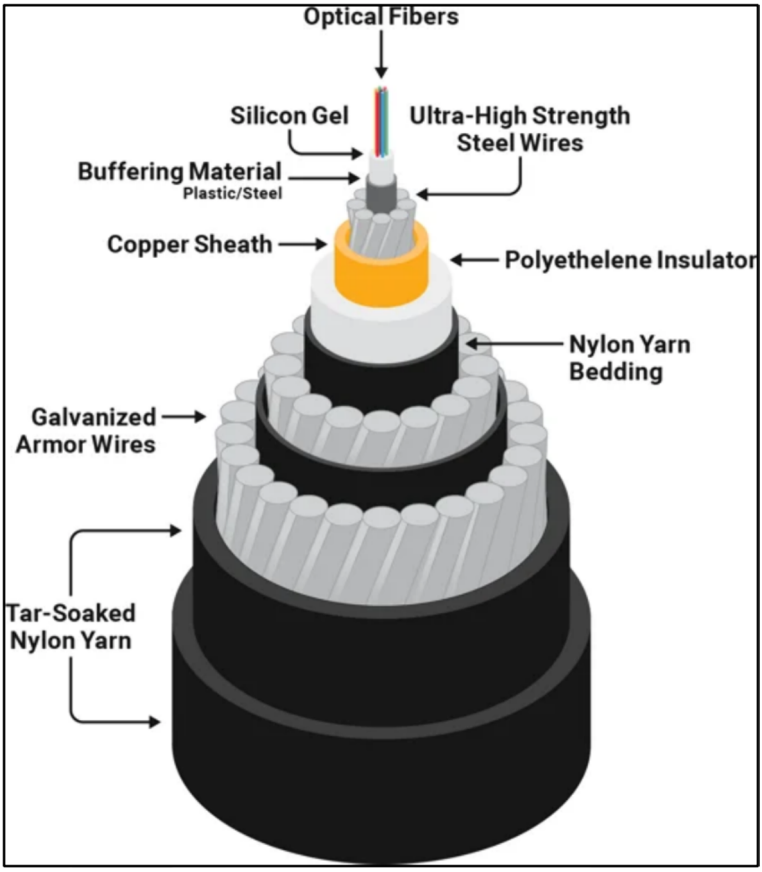

Fig. 3 A cross-section of a submarine cable. Source: telegeography.com under license CC BY-SA 4.0

export controls on chips to China (Bureau of Industry & Security, 2022). Indeed, China was suspected of intentionally cutting cables to a Taiwanese island group situated less than 20 kms off China's coast in early 2023 (Lii, 2023), which resulted in a 50-day internet outage (Braw, 2023).

Submarine cables can be easily cut since they generally have a minimum level of physical protection; the 1.4 million kilometres of cable globally are left unguarded and are typically only as thick as a garden hose, with a few centimetres of steel surrounding the fibre-optic cables in the core (Fig. 3). They are liable to damage, either by accident or intentional sabotage, so there is a continual risk to internet services. On average, there are over a hundred submarine cable faults each year, two-thirds due to ships' anchors or fishing (TeleGeography, 2023). In 2008, for example, a ship's anchor damaged the SEA-ME-WE 4 and FLAG cables near Alexandria, taking out as much as 70% of all internet and telephone traffic between Europe, Asia, and Africa (Johnson & Correspondent, 2008). The risk to submarine cables from intentional sabotage is likely much higher since the locations of most cables are public knowledge. However, it is also harder to determine due to states denying any accusations of sabotage.

Furthermore, it is unclear whether submarine cables are legitimate military targets during wartime, as they are dual-use objects.[1] Hence, there is a possibility that they would be targeted if they were seen to provide an advantage in a war. The first known example of a state actor destroying submarine communication cables during wartime occurred in the early hours of the 5th of August 1914, a few hours after England had declared war on Germany, when a British naval ship cut Germany's telecommunication cables (Winkler, 2008). NATO expects such attacks to continue in modern warfare, as evidenced by a 2010 document they published warning that submarine fibre-optic cable could be the target for attacks on the alliance (Morel, 2022). Although there are calls to protect cables during conflict (Kraska, 2020), it is unlikely that countries will agree to this, just as they have not agreed to protections for other combined civilian- and military-use infrastructure such as rail.

[1] While Art. 52 of the Geneva Convention states "In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage.", Art. 52.3 of the Geneva Convention states that "In case of doubt concerning an object that is normally used for civilian purposes—such as a house or other dwelling, a place of worship, or a school—parties to a conflict must assume that the object in question is not being used for military purposes". In general, several conditions must be satisfied for dual-use objects to be considered legitimate targets: purpose, effectiveness, definite military advantage, distinction, and proportionality. Moreover, if undersea cables connect non-belligerent countries, they may be considered immune under the Tallinn Manual (and Oslo Manual). Against this background, there is no clear-cut answer, and the subject is open to judicial interpretation.

4 Strategies for Digital Sovereignty Over Submarine Cables

Countries currently use three strategies to enhance their digital sovereignty over submarine cables and mitigate the risks outlined above. These are: regulatory controls, cable-building, and physical protection. Each of these three strategies protects against several of the risks just discussed.

4.1 Regulatory Controls for New Cables

Regulatory controls are generally used to constrain the influence of foreign nation-states on a country's SCI. They can lessen the risks of data interception by creating more robust controls on who has access to local traffic routes and the risk of losing control over technological infrastructure by reducing foreign actors' place in the infrastructure ecosystem. A variety of regulation methods for submarine cable control have been used: a requirement for regulatory approval when cable-laying, a requirement for regulatory approval when preparing for cable-laying, and conventional legal mechanisms such as tariffs and blacklisting.

As per Article 21(c) of UNCLOS, each country can set its own regulations regarding which actors can lay submarine cables in the territorial sea. This regulation can be used to control who may build, maintain, and own parts of the local SCI, thereby allowing a government to ensure that only companies it trusts, and/or it has sufficient control over, can participate in the local SCI. Due to submarine cables' multilateral and multi-stakeholder nature, this local regulation can also influence foreign countries and companies. The US and China provide clear examples of using regulatory approval for increasing SCI control. In 2021, Washington recommended that the Federal Communications Commission (FCC) grant Google and Meta approval to build a new submarine cable between the US, Taiwan, and the Philippines, only on condition that they agree to stringent national security terms about access to data and infrastructure from one of its financial backers based in Hong Kong (Goujard, 2021). In the case of China, its bar for regulatory approval is much higher than the US, as it prohibits any foreign telecom operations within its borders (Goodman & Wayland, 2022). This means that Chinese telecoms facilitate connectivity to the rest of the global internet using connection points that are physically located outside China's geographic borders. While this increases data security and control over technological infrastructure within China's borders, it is a less robust configuration for continued provision of service than the mixture of domestic and non-domestic connections seen in most other nations (Allen, 2019).

In contrast, the EU has not used the potential to create a regulatory regime for SCI approval. The EU provides a clear mechanism, in the form of the European Commission and Parliament, to allow landlocked states, such as Austria and Czechia, legislative power over the SCI. However, the EU currently leaves the authority to approve the laying of cables to individual Member States (Colombo et al., 2021), not taking advantage of its multinational nature.

A further regulatory means by which countries can govern the building of new cables is to use a regulatory approval regime for cable-laying preparations. Although

coastal countries that have ratified UNCLOS cannot prohibit other actors, like States, from laying cables (e.g. Article 79, UNCLOS), they can govern this process by regulating preparatory activities, such as prospecting and route planning. In fact, the combined provisions of Articles 56(1)(a), 58(3), and 79(3) and (4) of UNCLOS empower coastal States to determine the conditions under which submarine cables may be built within their exclusive economic zone and on their continental shelf, while also retaining jurisdiction over them even after construction. For example, China requires permits for seabed access within its exclusive economic zone, which allows it to supervise and exert influence over the organisations responsible for laying and managing the submarine cables. In 2023, China used this power to hold up the prospecting required for a new cable, SJC2, owned by a consortium including China Mobile and Meta, for several months due to espionage concerns (Gross et al., 2023a, 2023b). The permit requirement also ensures that China has complete control over its infrastructure and protects it against the risk of foreign actors having easy access to Chinese communications traffic. Furthermore, the approach protects against the risk of China diluting its control of cable standards since it provides Beijing with leverage to insist on its companies, vessels, or personnel being involved and having a seat at the table for infrastructure projects. This, in turn, gives China direct access to the international communications network.

Beyond the maritime regulatory approval regimes, countries also use conventional legal mechanisms to protect digital sovereignty concerning the SCI. For example, the EU used tariffs in 2021 as a defence mechanism against predatory pricing by foreign companies when an investigation had found that several Chinese companies, including Hengtong and Fiberhome Marine, were dumping fibre-optic cables into the European market at artificially low prices (Goodman & Wayland, 2022). Foreign-manufactured cables can be a risk to digital sovereignty since they could include backdoors that allow a third party to spy on data or shut it down remotely. Another conventional legal mechanism is blacklisting companies. Also in 2021, the US, for example, added several Chinese telecom and cabling companies to its trade blacklist, accusing them of attempting to acquire US technology, including HMN-Tech, which is majority owned by Hengtong, China's largest fibre-optic cable manufacturer (Goujard, 2021).

4.2 Cable Building

Building new cables via a government-owned company, or allying with private companies in the cable-building industry, works to protect a country's digital sovereignty by increasing that country's influence over the SCI. If a country builds new cables, this mitigates the risk of other countries intercepting its data and gives its government control (potentially via private companies) over the cable's usage. Consequently, this diminishes foreign influence and power over the country's technological infrastructure. In a reciprocal dynamic, nations, aware of the susceptibility to foreign influence and data espionage stemming from reliance on foreign submarine cables, strategically construct their own cables to gain these capabilities themselves.

Laying one's own cable allows one to bypass potential cable-tapping in two ways. Firstly, a new submarine cable could enable a country, whether landlocked or coastal, to avoid routing data through an unwanted country, thereby avoiding the possibility of them cutting off or tapping the data. The EU, for example, in light of the war in Ukraine, is exploring the possibility of laying a new cable through the Black Sea between Georgia and Eastern Europe, bypassing Russia. This would guarantee the independence of internet connections from pre-existing infrastructure on Russian territory (Gross, Campbell, and Heal 2023a). Secondly, countries, or companies under a nation's direct or indirect control, will have exclusive control over cable landing points within their territorial boundaries. China's Digital Silk Road (DSR), launched in 2015, aims to capitalise on both benefits with plans to own, design, operate, and control digital connectivity infrastructure to achieve greater technological independence and influence (Ghiasy, 2020).

Beyond defending against wiretapping, building submarine cables allows a country control over data-routing. This means that the country can prioritise specific routes or destinations for data traffic, potentially giving preference to critical national interests or security requirements. This is complicated, however, if it is not a state or state-owned company that owns the cables, but a private company. In this case, the relationship between the company and the state is crucial, as differing priorities may undermine the country's ability to exercise complete control over data routing.

A final defensive advantage of building new cables is that they allow countries to provide greater stability in their service provision. Network resilience is significantly increased if a country has multiple submarine cables connecting it to any given destination instead of a single one, as this builds redundancy and diversity into the network. The growth of the satellite telecommunications network in recent years could provide an alternative telecommunication pathway. However, as noted above, its current capacity cannot bear even a tenth of the submarine cable traffic. Egypt is a prominent illustration in this regard: 10 of the 11 cables that pass through it from the Mediterranean are duplicated. Both the number of different cables and the duplication ensure diverse and redundant routes, which bolsters network resilience. However, the large number of cables is mainly down to foreign interest in passing through the Red Sea rather than Egypt's own initiative.

As so much of the SCI infrastructure is private, governments can increase their influence by allying more closely with related private companies. There are multiple stages in the construction of submarine cables in which companies are involved: the manufacturing, laying, maintenance, and ownership of the cables. By allying more closely with companies at each stage, a government can increase its influence over the local SCI and its digital sovereignty, as it has greater influence over landing points, data routing, and technical standards. For example, closer involvement with cable manufacturing allows a government to dictate the standards of the cable, even outside of their legislative borders; hence China's *Made in China 2025* strategic plan, which aspires to secure Chinese control over 60 per cent of the global fibre-optic market by 2025 (Rossiter, 2023). It is not by chance that five of the seven major fibre-optic cable companies in the world are Chinese, including Huawei, ZTE, and China Telecom (Bechis, 2021).

Building submarine cables should not be seen as a wholly defensive strategy by which countries only shore up their digital sovereignty against foreign influence. Countries are just as willing to use submarine cables to exert influence and dependency upon foreign states. Coastal countries, for example, can not only control landing points on their shores and legislate cables that make landfall (assuming the cables were not built before the ratification of UNCLOS), but they can also become a node on which other countries rely. The greater the number of cables they build to other countries, the more such countries will depend on them.

Occupying a central position within the global submarine cable network allows for countries to utilise weaponised interdependence (Farrell & Newman, 2019), as discussed in reference to companies in Sect. 2.2. Some coastal countries are naturally well-placed to enact this strategy, working as central nodes through which a significant amount of telecommunications traffic travels. Ireland, for example, has three-quarters of all cables in the northern hemisphere passing through or near its waters (McCabe & Flynn, 2024) and the submarine cables traversing Egypt's waters are used by one-third of the global internet due to its position at the intersection of Asia, Africa, and Europe, controlling the Suez Canal (Aldrich & Karatzogianni, 2020). Egypt is capitalising on its position as the shortest and most reliable path between Europe, Asia, and Africa (Fig. 4) (Eldahshory & Khaled, 2021), ensuring it retains influence over most of the 11 cables passing through the Suez Canal and Red Sea corridor, with 79–84%[2] of the cables at least partially owned by Telecom Egypt (TE) and 70% of TE owned by the Egyptian government. This gives the Egyptian government substantial leverage over critical communication infrastructure. Other countries and companies are responding to this dependence on TE and hence potentially weaponised interdependence by exploring alternative routes. Google has successfully pursued the option of its Blue-Raman cable via Israel as a means to bypass Egypt (Burgess, 2022) and other parties are exploring terrestrial routes through Central Asia and Russia (Qiu, 2020).

Even non-central countries can use this strategy for weaponised interdependence, as any government can build or invest in cables that never land on their own shore. This allows them to directly intervene in developing third-country cables, encompassing regulatory determinations concerning cable access and international routes (McGeachy, 2022). China's DSR initiative, for example, also assists in building telecommunication networks in recipient states, just as Google's Equiano cable noted in Sect. 2.1. In general, it can be seen from Fig. 1 that the global north has used its power over the construction of submarine cables to create a telecommunications infrastructure in which South America and Africa are extensions of the northern network rather than equivalent regions (Pérez, 2023). This creates an unequal power dynamic and information flow forcing countries in the global south to rely on the global north for connectivity.

[2] The owners of one Red Sea cable have not been made public.

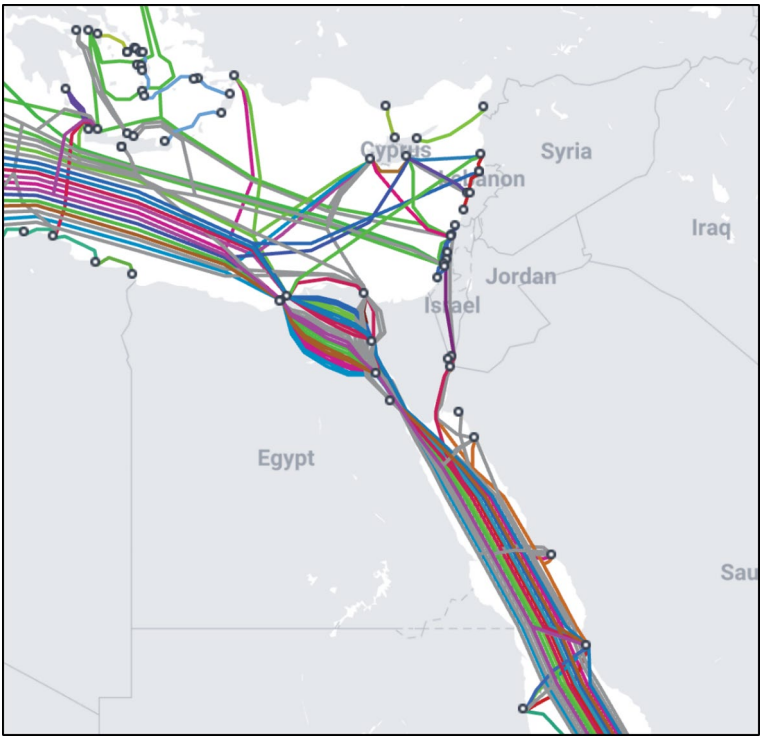

Fig. 4 The 14 in-service and six planned cables that have landing points in Egypt. Source: telegeography.com under license CC BY-SA 4.0

4.3 Protection of Pre-existing Cables

The third and final strategy that countries are currently using to mitigate the risk to their digital sovereignty is increasing the level of protection of submarine cables. This is intended to defend against the risk of wiretapping and the risk to a country's ability to provide internet-reliant services.

Unfortunately, with the longest cables running to 20,000 km (TeleGeography, 2023), increasing a cable's physical protection can be cost-prohibitive. The cost can be drastically reduced by focusing on the most vulnerable parts of the cable, meaning those closest to the shore and, hence, within legislative boundaries. For example, New Zealand, Australia, Uruguay, and Colombia have adopted cable protection legislation. New Zealand and Australia, in 1996 and 2007, respectively, created cable protection zones along cable routes, extending from the shore to a water depth of 2000 m (Australian Government, 2008; New Zealand Government, 1996). These restrictions are intended to protect against accidental damage by restricting activities that could pose a risk to the cables. However, the legal basis for such protection zones outside of territorial seas (as in the case of Australia) has been questioned (Kaye, 2008; Liao, 2019), with the International Law Commission declaring in 1956

that such zones "would constitute a further encroachment on the freedom of navigation and fishing" (Yearbook of the International Law Commission12, 1956). Nevertheless, no legal challenge to the legislation has yet arisen, and states continue to implement the legislation.

Besides legislative routes, one can also increase the direct protection around individual cables. One proposal in this domain is to use sensors to detect submarines or other potential dangers. These sensors could either be part of the cable itself (Eleftherakis & Vicen-Bueno, 2020) or a separate network (Wong, 2016). However, Bueger et al. suggest that by equipping submarine cables with the technology to detect submarines, cables would undermine their dual-use nature and make them valid military targets, putting civilian use at risk (Bueger et al., 2022). Alternatively, the UK has invested in a surveillance ship for underwater infrastructure, particularly submarine cables (Ministry of Defence and Wallace, 2021). It is worth noting, however, that neither of these methods is feasible for the largest-scale submarine cables due to prohibitive costs.

5 Limitations of Current Mechanisms

Current methods for digital sovereignty over the SCI fall short. Rerouting data around a hostile state cannot protect against information interception, only four countries have protection zones around cables, and lack of global cooperation between states cedes technological control to third parties.

While countries wish to maintain data privacy, protecting cables from physical wiretapping is infeasible: the high cost of implementing comprehensive protection measures to restrict unauthorised access and the complex multi-stakeholder nature of transnational cables make ensuring access solely to trusted entities challenging. However, preventing potential adversaries from deciphering the extracted information is still feasible. Countries should focus on increasing the proportion of encrypted internet traffic by promoting the adoption of secure protocols such as HTTPS for websites and advocating for encryption services across all communication platforms, including email providers. For highly classified communications, it is crucial to emphasise the use of quantum-safe encryption algorithms, i.e. encryption that quantum computers cannot easily decrypt. Already existing and implemented quantum-resistant algorithms are gradually being incorporated into current policies, with organisations like NIST planning to release a post-quantum cryptographic standard by 2024 ('NIST Announces First Four Quantum-Resistant Cryptographic Algorithms' 2022). While the current speed and computational cost of quantum-safe encryption make it impractical for everyday usage, its adoption is imperative for communications that would pose a risk if decrypted in the future.

To ensure the provision of internet-reliant services, two mechanisms are currently used: protecting the cable from physical damage and increasing the diversity of cables. Both mechanisms are valuable but have yet to be widely adopted, leaving room for a third approach. Current methods for protecting the cable from physical damage provide inadequate protection, as shown by the hundreds of accidental faults occurring each year and the possibility of intentional damage being inflicted

very easily. Given the cable length and the cost of increasing physical protection or surveillance, a much higher degree of direct protection is infeasible.

Nevertheless, much could be done to improve protection from at least accidental harm. 57% of cable faults are caused by anchorage and fishing, generally near the shore. Costs can be significantly reduced by increasing protection only for this part of the cable, which in turn would mitigate the economic impacts of internet outages. These parts of the cable already have increased physical protection, with the diameter of a cable increasing from one inch in the deep sea to four and a half inches near the shore. An alternative to adding more padding to the cable is to extend the protection zones used by countries such as Australia (see Sect. 4). Protection zones appeal on the basis that they do not require any additional physical material for the cable, or modification of already laid cables. Thus far, they have been implemented only by four countries (New Zealand, Australia, Uruguay, and Colombia). These zones can either be discretionary (e.g. Australia) or mandatory (e.g. New Zealand) depending on whether cable operators are allowed to lay cables outside of the protection zones. Submarine cable operators are not in favour of protection zones when they are mandatory. This causes grouping of cables which operators argue makes installation and maintenance more difficult (due to the danger of damaging other cables) and makes cables more vulnerable to attack (ICPC, 2023), as can be seen from an incident in March 2024 where three cables running through the red sea were cut simultaneously (Gambrell, 2024). Nevertheless, discretionary cable protection zones can be implemented by further countries where possible, even taking into account the discussion around their legality beyond territorial seas (Guilfoyle et al., 2022). If cables intersect busy shipping lanes or ports adopting this policy is more difficult. For countries like Egypt, which have submarine cables passing through important shipping lanes, alternative protection mechanisms should be found, such as the duplication of cables. In the latter case, where the submarine cables land near ports, we strongly advise new routes for future cables.

The alternative approach is to increase the diversity of cables, that is, increase the number of cables and routes between two end-points or through the same stretch of water. This augmentation increases the network's resilience. For example, in areas of intense maritime activity such as the Suez Canal, implementing various cables and routes mitigates the potential loss of network capacity due to anchorage damage. As more stand-alone submarine cables are built, the diversity of cables available also increases. However, cables stemming from current investments are not built to add redundancy to the network but are responding to the growing demands of internet use, meaning that overall network resilience is not increased sufficiently.

One alternative to increasing the number of cables is increasing the diversity of communication methods which also increases the capacity for data transmission in general. Currently, the only clear alternative to submarine cables are satellites. They have not previously attracted as much investment since, as of 2022, satellite networks have latency 10% higher than terrestrial transfer on average, with 3.8 times as much variation, and transfer speeds which are slower by half (Ma et al., 2022). Further, they result in space debris (Byers & Boley, 2023; Kessler & Cour-Palais, 1978), which is not easy to remove and poses a risk to other satellites. Nevertheless, they are a viable alternative. Currently, the push towards and investments in satellite

communications come primarily from private companies such as Starlink. To avoid constant regulatory catch-up and allow countries to maintain some control over their technological infrastructure, governments and regional organisations should themselves invest in satellite communications and proactively establish an international forum for this technology that acts as a counterpart to the ICPC. This sister organisation should aim to engage with all stakeholders in the satellite communications sector, to foster the exchange of technical, legal, and environmental information.[3] One of its responsibilities would be to decide which traffic would be taken up by satellites in the case of cable failure—the priority of different traffic is a matter for governments to decide.

Finally, countries' current mechanisms to achieve greater control over technological infrastructure lack coordination and are non-existent for any country with no landing points nor cable ownership. There are multiple ways in which both of these gaps can be targeted. First, to increase coordination, previously extant international alliances and forums should be used for submarine cable governance. The ICPC, for example, should not remain predominantly a forum for companies with only a few government representatives. Instead, since all governments rely on submarine cables, they should join the ICPC regardless of cable ownership or coastal presence, and, in turn, the ICPC should give them a recognised voice at meetings. Second, there is a clear gap for supranational bodies, including the European Union, to develop collective-wide regulation on submarine cables. This approach would allow individual countries to continue investing in and ensuring the development of new cables while also providing a platform for non-owner countries to have a voice and influence over the submarine cables on which they depend. By allowing and inviting all countries to cooperate on technological standards and developments for submarine cables, power will be moved from the hands of companies, which currently own most cables, into the hands of governments and citizens. This will likely result in a pushback from companies, which may have concerns about increasing government regulation leading to increased costs and delays associated with regulatory compliance. As can be seen from the discussion of mandatory protection zones above, even regulations aimed at protecting submarine cables may cause discontent among cable operators. While this strategy has its distinctive risks, it has the potential to rebalance the distribution of power and control over SCI.

6 Conclusion

There has been a blasé attitude to the SCI and its ownership. The multinational nature of submarine cables, combined with their joint existence in different legal jurisdictions and the joint private–public ownership of submarine cables, makes governance difficult. Furthermore, given the limits of current technology, some risks are impossible to combat cost-effectively—not every metre of cable can be protected

[3] Currently, there exists the International Telecommunications Satellite Organization. However, this governs only Intelsat and does not include projects such as Starlink.

from damage or wiretapping. These challenges have resulted in countries accepting the slide towards private ownership of the SCI, justified in that belief by the fact that much infrastructure has private ownership. However, there are two key differences for the SCI. First, it is a critical infrastructure, even if its absence does not immediately lead to physical harm. Second, while other infrastructure is often owned by private companies, it is not usually owned by *foreign* private companies, nor by companies whose nation-states have expressed an explicit interest in extending their foreign power via internet infrastructure. Thus, many countries are actively not responding to intentional international infringements on their digital sovereignty. This is not to say that all foreign-owned cables should be cut; it is inefficient for every country to own a submarine cable for every continent, and the global internet is necessarily multinational. Rather, governments should direct foreign investment towards home-grown companies, ensure that submarine cables are owned by consortia, which include local companies or government, and use international organisations such as the EU or African Union. In conjunction with this, all data should be encrypted post-haste and the most sensitive data with quantum-safe encryption schemes, to defend against current and future wiretapping. In these ways, despite the SCI's inherent challenges to unilateral governance, countries can retain a degree of control over their infrastructure.

Acknowledgements We are grateful to Tyler Schroder for his contributions to this paper. Martina Camellini's and Claudio Novelli's contributions were supported by funding provided by the Vodafone Institute to the University of Bologna.

References

Aldrich, R. J., & Karatzogianni, A. (2020). Postdigital war beneath the sea? The Stack's underwater cable insecurity. *Digital War, 1*(1), 29–35. https://doi.org/10.1057/s42984-020-00014-x

Allen, D. (2019). 'Analysis by Oracle Internet Intelligence Highlights China's Unique Approach to Connecting to the Global Internet | Internet Intelligence - Powered by Oracle Cloud Infrastructure'. 2019. https://web.archive.org/web/20210514052906/https://blogs.oracle.com/internetintelligence/analysis-by-oracle-internet-intelligence-highlights-china%e2%80%99s-unique-approach-to-connecting-to-the-global-internet.

Aluf, D. (2023). 'China's Subsea-Cable Power in the Middle East and North Africa'. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinas-subsea-cable-power-in-the-middle-east-and-north-africa/.

Angwin, J., Savage, C., Larson, J., Moltke, H., Poitras, L., Risen, J. (2015). 'AT&T Helped U.S. Spy on Internet on a Vast Scale'. *The New York Times*, Retrieved August 15, 2015, from https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html.

Australian Government. (2008). *Submarine Cable (Perth Protection Zone) Declaration 2007*. Attorney-General's Department. https://www.legislation.gov.au/Details/F2007L03914/Html/Text, http://www.legislation.gov.au/Details/F2007L03914.

Bechis, F. (2021). 'Undersea Cables: The Great Data Race Beneath the Oceans'. *ISPI* (blog). Retrieved May 28, 2021, from https://www.ispionline.it/en/publication/undersea-cables-great-data-race-beneath-oceans-30651.

Braw, E. (2023). 'China Is Practicing How to Sever Taiwan's Internet'. *Foreign Policy* (blog). Retrieved February 21, 2023, from https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/.

Brock, J. (2023). 'U.S. and China Wage War beneath the Waves - over Internet Cables'. *Reuters*, Retrieved May 27, 2023, from https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

Bueger, C., Liebetrau, T., Franken, J. (2022). *Security Threats to Undersea Communications Cables and Infrastructure—Consequences for the EU*. https://doi.org/10.13140/RG.2.2.21564.31365.

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy, 42*(3), 391–413. https://doi.org/10.1080/13523260.2021.1907129

Bureau of Industry and Security. (2022). 'Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)'. Bureau of Industry and Security, U.S. Department of Commerce. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file.

Burgess, M. (2022). 'The Most Vulnerable Place on the Internet'. *Wired*, Retrieved November 2, 2022, from https://www.wired.com/story/submarine-internet-cables-egypt/.

Byers, M., & Boley, A. (2023). Who owns outer space?: International law, astrophysics, and the sustainable development of space. *Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press*. https://doi.org/10.1017/9781108597135

Carr, M. (2015). Power plays in global internet governance. *Millennium, 43*(2), 640–659. https://doi.org/10.1177/0305829814562655

Colombo, M., Solfrini, F., Varvelli, A. (2021). 'Network Effects: Europe's Digital Sovereignty in the Mediterranean'. European Council on Foreign Relations. https://www.jstor.org/stable/resrep32468.

Eldahshory, M., Khaled, O. (2021). 'STF Mag Feature: Telecom Egypt's Infrastructure'. *SubTel Forum* (blog). Retrieved November 30, 2021, from https://subtelforum.com/stf-mag-feature-telecom-egypts-infrastructure/.

Eleftherakis, D., & Vicen-Bueno, R. (2020). Sensors to increase the security of underwater communication cables: A review of underwater monitoring sensors. *Sensors, 20*(3), 737. https://doi.org/10.3390/s20030737

European Commission. (2024). 'Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures'. Retrieved February 26, 2024, from https://www.eesc.europa.eu/en/documents/commission-recommendation-2622024-secure-and-resilient-submarine-cable-infrastructures.

Farrell, H., Newman, A. L. (2019). 'How Global Economic Networks Shape State Coercion'.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology, 33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Frazier, K. (2023). 'On Protecting the Undersea Cable System'. Lawfare. 12 January 2023. https://www.lawfareblog.com/protecting-undersea-cable-system.

Gambrell, J. (2024). '3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway'. *AP News*. 4 March 2024.

Ghiasy, R. (2020). 'China's Digital Silk Road'.

Gjesvik, L. (2023). Private infrastructure in Weaponized interdependence. *Review of International Political Economy, 30*(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145

Goodman, M. P., Wayland, M. (2022). 'Securing Asia's Subsea Network'.

Google. (2023). 'Google Transparency Report'. Retrieved November 8, 2023, from https://transparencyreport.google.com/https/overview?hl=en.

Goujard, C. (2021). 'Finnish-US Internet Cable Planned to Bolster Europe's Digital Trade with Asia'. *POLITICO* (blog). Retrieved December 22, 2021, from https://www.politico.eu/article/finnish-us-internet-cable-europe-digital-trade-asia/.

Gross, A., Sevastopulo, D., Ruehl, M., Hille, K., Heal, A. (2023b). 'China Exerts Control over Internet Cable Projects in South China Sea'. *Financial Times*, 13 March 2023, sec. Chinese politics & policy. https://www.ft.com/content/89bc954d-64ed-4d80-bb8f-9f1852ec4eb1.

Gross, A., Campbell, C., Heal, A. (2023a). 'EU Plans Black Sea Internet Cable to Reduce Reliance on Russia'. *Financial Times*, 12 May 2023, sec. Infrastructure investment. https://www.ft.com/content/d07dbd19-5e8b-4543-85f6-bbf1a6a0858d.

Guilfoyle, D., Paige, T. P., & McLaughlin, R. (2022). The final frontier of cyberspace: The seabed beyond national jurisdiction and the protection of submarine cables. *International & Comparative Law Quarterly, 71*(3), 657–696. https://doi.org/10.1017/S0020589322000227

Hoffman, D. (2010). *The dead hand: The untold story of the cold war arms race and its dangerous legacy*. Knopf Doubleday Publishing Group.

ICPC. (2023). 'Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables'. 4 October 2023.

Johnson, B., Technology correspondent. (2008). 'Internet Connection Cut between Europe, Asia and Africa'. *The Guardian*, 21 December 2008, sec. World news. https://www.theguardian.com/world/2008/dec/21/internet-cable-cut.

Kaye, S. (2008). 'The Protection of Platforms, Pipelines and Submarine Cables under Australian and New Zealand Law'. *Australian and New Zealand Maritime Law Journal*, November. https://maritime.law.uq.edu.au/index.php/anzmlj/article/view/2095.

Kessler, D. J., & Cour-Palais, B. G. (1978). Collision frequency of artificial satellites: The creation of a debris belt. *Journal of Geophysical Research: Space Physics, 83*(A6), 2637–2646. https://doi.org/10.1029/JA083iA06p02637

Kramer, D. (2023). The future has arrived for securing confidential data. *Physics Today, 76*(11), 21–24. https://doi.org/10.1063/PT.3.5340

Kraska, J. (2020). 'Submarine Cables in the Law of Naval Warfare'. Default. Retrieved July 10, 2020, from https://www.lawfaremedia.org/article/submarine-cables-law-naval-warfare.

Let's Encrypt. (2023). 'Let's Encrypt Stats'. Let's Encrypt. Retrieved November 8, 2023, from https://letsencrypt.org/stats/.

Liao, X. (2019). Protection of submarine cables against acts of terrorism. *Ocean Yearbook Online, 33*(1), 456–486. https://doi.org/10.1163/9789004395633_018

Lii, W. (2023). 'After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience'. Retrieved April 15, 2023, from https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/.

Liu, S., Bischof, Z. S., Madan, I., Chan, P. K., Bustamante, F. E. (2020). 'Out of sight, not out of mind: a user-view on the criticality of the submarine cable network'. In *Proceedings of the ACM Internet Measurement Conference*, 194–200. Virtual Event USA: ACM. https://doi.org/10.1145/3419394.3423633.

Ma, S., Ching Chou, Y., Zhao, H., Chen, L., Ma, X., Liu, J. (2022). 'Network Characteristics of LEO Satellite Constellations: A Starlink-Based Measurement from End Users'. arXiv. https://doi.org/10.48550/arXiv.2212.13697.

Mauldin, A. (2023). 'Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?' Retrieved May 4, 2023, from https://blog.telegeography.com/2023-mythbusting-part-3.

McCabe, R., & Flynn, B. (2024). Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure. *European Security, 33*(2), 324–344. https://doi.org/10.1080/09662839.2023.2248001

McGeachy, H. (2022). The changing strategic significance of submarine cables: Old technology, new concerns. *Australian Journal of International Affairs, 76*(2), 161–177. https://doi.org/10.1080/10357718.2022.2051427

'Member List'. 2023. Retrieved November 6, 2023, from https://www.iscpc.org/about-the-icpc/member-list/.

Ministry of Defence, Wallace, B. (2021). 'New Royal Navy Surveillance Ship to Protect the UK's Critical Underwater Infrastructure'. GOV.UK. 24 March 2021. https://www.gov.uk/government/news/new-royal-navy-surveillance-ship-to-protect-the-uks-critical-underwater-infrastructure.

Morel, Camille. 2022. 'Les cables sous-marins : un bien commun mondial ?'

New Zealand Government. 1996. *Submarine Cables and Pipelines Protection Act 1996*. https://www.legislation.govt.nz/act/public/1996/0022/latest/DLM375803.html.

BBC News. 2022. 'Nord Stream 1: How Russia Is Cutting Gas Supplies to Europe', 27 January 2022, sec. Europe. https://www.bbc.com/news/world-europe-60131520.

'NIST Announces First Four Quantum-Resistant Cryptographic Algorithms'. 2022. *NIST*, July. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

O'Carroll, E. (2021). 'Google's Equiano Subsea Cable: Regional Economic Impact Assessment'. Africa Practice. Retrieved October 5, 2021, from https://africapractice.com/insights/equiano-reia/.

Pérez, R. G. (2023). *Submarine cables across the Atlantic: Geopolitics and security of a critical infrastructure*. Atlantic Centre.

Qiu, W. (2020). 'A study on submarine cables crossing Egypt and their costs—submarine networks'. Retrieved April 22, 2020, from https://www.submarinenetworks.com/en/services/research/submarine-cables-crossing-egypt-and-cost.

Roberts, H., Hine, E., Floridi, L. (2023). 'Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance'. In *Quo Vadis, Sovereignty? : New Conceptual and Regulatory*

Boundaries in the Age of Digital China, edited by Marina Timoteo, Barbara Verri, and Riccardo Nanni, 51–75. Philosophical Studies Series. Springer. https://doi.org/10.1007/978-3-031-41566-1_4.

Rossiter, A. (2023). 'TRENDS Research & Advisory Strives to Present an Insightful and Informed View of Global Issues and Challenges from a Strategic Perspective.' Trends Research. Retrieved February 19, 2023, from https://trendsresearch.org/index.html.

Satariano, A., Russell, K., Griggs, T., Migliozzi, B., Lee, C. W. (2019). 'How the Internet Travels Across Oceans'. *The New York Times*, 10 March 2019, sec. Technology. https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html.

Sherman, J. (2021). *Cyber defense across the ocean floor*. Atlantic Council.

Suganami, H., Carr, M., & Humphreys, A. R. C. (2017). *The anarchical society at 40: Contemporary challenges and prospects*. Oxford University Press.

Tedeschi, P., Sciancalepore, S., & Di Pietro, R. (2022). Satellite-based communications security: A survey of threats, solutions, and research challenges. *Computer Networks, 216*(October), 109246. https://doi.org/10.1016/j.comnet.2022.109246

TeleGeography. (2023). 'Submarine Cable FAQs'. Retrieved November 6, 2023, from https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

Tretter, M. (2022). Sovereignty in the digital and contact tracing apps. *Digital Society, 2*(1), 2. https://doi.org/10.1007/s44206-022-00030-2

US Department of Commerce, National Oceanic and Atmospheric Administration. 2023. 'What Is the Law of the Sea?' Retrieved August 15, 2023, from https://oceanservice.noaa.gov/facts/lawofsea.html.

Werr, P. (2023). 'Egypt Sells $121.6 Mln Stake in State-Controlled Telecom Egypt'. *Reuters*, 14 May 2023, sec. Deals. https://www.reuters.com/markets/deals/egypt-sells-1216-mln-stake-state-controlled-telecom-egypt-2023-05-14/.

Winkler, J. R. (2008). *Nexus: Strategic Communications and American Security in World War I: 162* (1st ed.). Harvard University Press.

Wong. (2016). '"Underwater Great Wall": Chinese Firm Proposes Building Network of Submarine Detectors to Boost Nation's Defence'. South China Morning Post. Retrieved May 19, 2016, from https://www.scmp.com/news/china/diplomacy-defence/article/1947212/underwater-great-wall-chinese-firm-proposes-building.

Yearbook of the International Law Commission 12. 1956. Vol. 2.