SUBMARINE CABLES: THE CHANGING STRATEGIC SIGNIFICANCE OF A HIDDEN INFRASTRUCTURE

Edoardo Maria Landoni

Until recently, the fibre-optic cables laid on the seabed received relatively little public and political attention, despite constituting the physical backbone of global connectivity. This limited visibility has itself been the subject of scholarly inquiry. Christian Bueger and Tobias Liebetrau, in particular, have explained it through the concept of "triple invisibility". First, submarine cables share a characteristic common to infrastructures more generally: they tend to recede into the background of everyday life, becoming noticeable primarily when they cease to function. Second, their location beneath the surface of the water places them outside ordinary observation and, consequently, much of public debate. Third, they are situated at sea, a space that policy debates have historically tended to regard as relatively empty and distant from political governance. This invisibility has been reinforced by popular representations of the internet as a predominantly wireless system, sustained by satellites and an apparently immaterial "cloud", which obscure its dependence on an extensive physical infrastructure extending across the ocean floor.

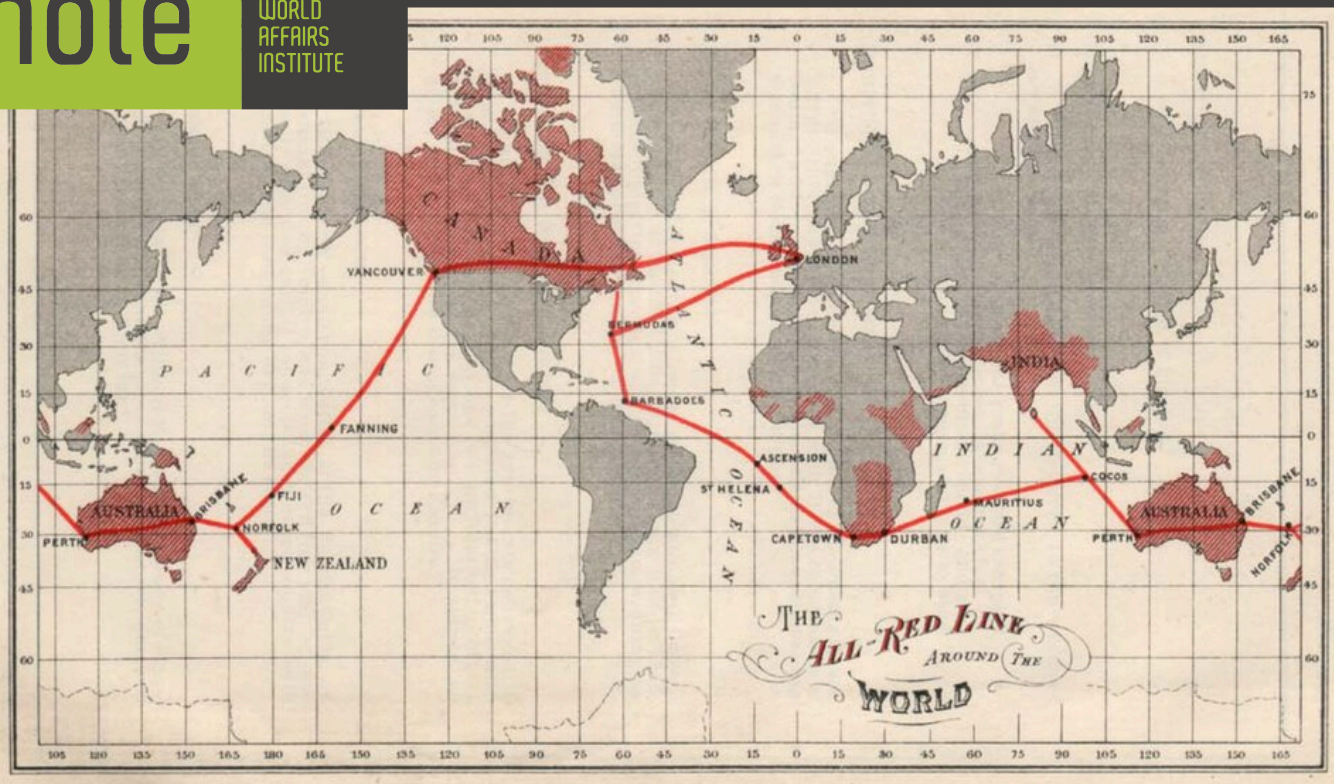
In recent years, however, a series of incidents has brought submarine cables increasingly into public debate and security policy. In February 2024, three cable systems in the Red Sea were severed, most likely by the dragging anchor of the *Rubymar*, a cargo ship that had been struck by a Houthi missile and subsequently abandoned by its crew. According to the estimate of one operator, the incident affected approximately a quarter of data traffic between Asia and Europe. In September 2025, further cable cuts off Jeddah disrupted connectivity across the Gulf and South Asia, prompting Microsoft to warn its cloud customers of increased latency. In the Baltic Sea, a series of incidents involving the dragging of anchors across data and power cables led NATO to establish a dedicated surveillance activity, Baltic Sentry, and the European Union to adopt an Action Plan on Cable Security. Comparable incidents have also occurred around Taiwan and, in August 2026, within a cable protection zone off Perth, where two cables were damaged in quick succession.

These incidents nevertheless require a cautious interpretation. Cable faults are a relatively common occurrence. The International Cable Protection Committee reports approximately 150 to 200 faults annually, attributing between 70 and 80 percent of them to accidental causes, primarily fishing activities and anchoring. Even in several recent cases, deliberate intent has been difficult to establish and responsibility remains uncertain. The significance of these developments therefore lies less in evidence of an increased frequency of damage than in the changing political interpretation of such incidents. Cable failures, previously approached predominantly as technical and commercial problems involving operators, engineers and insurers, are increasingly assessed in relation to possible state involvement and their implications for national security, often being framed as acts of *hybrid warfare*, a widely used but loosely defined concept.

The scale and geographical configuration of the submarine cable network help explain its growing strategic relevance. TeleGeography currently identifies 607 cable systems in service and approximately one hundred more under development, forming a network extending over 1.5 million kilometres. These cables carry more than 95 percent of intercontinental data traffic, while satellites continue to play a comparatively limited, complementary role. The network, however, is highly uneven in its geographical distribution. Cables are concentrated along a relatively small number of corridors, particularly the North Atlantic, the Mediterranean, the Red Sea, the waters surrounding Singapore and the South China Sea, and the North Pacific. Their distribution largely follows established maritime routes, reflecting the influence of geographical distance on construction costs and transmission latency. Connections between Europe and Asia, for instance, generally pass through Suez and the Bab el-Mandeb rather than circumnavigating Africa. As a consequence, submarine telecommunications are exposed to many of the same geographical chokepoints that have historically shaped maritime trade. The Red Sea offers a particularly clear example since more than a dozen cables pass through a narrow, shallow and heavily trafficked corridor, adjacent to an area of ongoing armed conflict. Shallow waters also increase their exposure both to accidental damage from anchoring and to potential deliberate interference.

tnote
TORINO WORLD AFFAIRS INSTITUTE

Sketch map of the All Red Line drawn in 1902-1903 Source: Wikicommons



Understanding the strategic significance of these vulnerabilities may require placing submarine communications within a longer historical perspective. Although fibre-optic technology is relatively recent, undersea telecommunications have a history extending back to the nineteenth century. This development can be divided into four broad phases, each associated with distinct technologies, arrangements of ownership and governance, and more importantly different conceptions of strategy and security.

The history of submarine cables extends much further back than one might expect, beginning in the nineteenth century with the development of telegraph networks. A copper telegraph cable was laid across the English Channel in 1850, while the first durable transatlantic connection was established in 1866. Britain, which dominated both cable manufacturing and the supply of gutta-percha, the natural material used to insulate submarine cables, progressively incorporated submarine communications into its imperial strategy. As Paul Kennedy demonstrated in his study of British cable communications, imperial planners regarded dependence on landlines crossing foreign territories as a potential source of vulnerability, since such connections could be intercepted or interrupted during an international crisis. This concern contributed to the development of the All-Red Line, a global telegraph network completed in 1902, whose landing points were situated exclusively within British territories. At the same time, British authorities maintained detailed information on foreign cable networks and on the connections whose interruption would be necessary to isolate potential adversaries. The strategic importance of submarine cables became particularly evident during the First World War. In August 1914, shortly after the outbreak of hostilities, Britain cut Germany's submarine cables, disrupting its international communications. In 1917, British control over cable routes also enabled the interception of the Zimmermann telegram, a secret German diplomatic message transmitted through a cable passing through British territory. These emblematic episodes illustrate how control over submarine communication networks could serve both to restrict an adversary's communications and to intercept sensitive information, and they show how security was understood primarily in terms of control over cable routes and landing points.

> "The current transformation of the international order has, however, brought the geopolitical dimension of submarine communications back to the fore."

A second phase, extending roughly from the mid-1950s to the late 1980s, can be associated with the introduction of a new technology, that of coaxial cables. At the same time, the emergence of the Cold War order contributed to a reorganisation of submarine telecommunications. Submarine cables were jointly owned and operated by groups of national telecommunications carriers, generally aligned with their respective governments, which shared construction costs, landing rights and revenues within the framework of Cold War blocs. Security considerations thus remained central, although they changed shape as they had to deal with the threat of nuclear conflict. This was reflected in the emphasis placed on network redundancy and in the choice of landing sites in peripheral areas, away from potential military targets.

The third phase then corresponds to the introduction of fibre-optic technology and the liberalisation of telecommunications markets. From the late 1980s, the transmission of information through pulses of light carried by glass fibres increased communication capacity by several orders of magnitude, providing the technical foundation for the expansion of the commercial internet. At the same time, liberalisation and privatisation progressively transformed the institutional organisation of the industry, weakening the consortium model that had characterised the Cold War period, while private companies increasingly determined cable routes and landing points according to market demand.

Within the broader political context of the post-Cold War period, submarine cables came to be conceived primarily as commercial infrastructures supporting economic globalisation. Questions of security were increasingly expressed in terms of operational reliability, service continuity and risk management rather than territorial control or geopolitical competition. The relative invisibility of submarine cables described earlier can therefore be understood as a historically specific development, associated with a period in which their strategic significance became less prominent in public policy and political debate.

Finally, a fourth phase can be identified in the current transformation of the international order, which has brought the geopolitical dimension of submarine communications back to the fore. As the liberal international order that emerged after the Cold War has progressively weakened, so too has the assumption that growing interdependence would necessarily foster integration and stability. Instead, interdependence has increasingly come to be regarded as a potential source of vulnerability, and the infrastructures sustaining it as potential instruments of political and strategic leverage. In this context, security concerns that had shaped submarine cable networks during the imperial and Cold War periods have regained importance. The difference, however, is that these concerns now apply to a network largely developed under the commercial logic of the post-Cold War era, when economic efficiency and global connectivity had taken precedence over geopolitical considerations.

In 2020, for example, a US interagency committee recommended that the Federal Communications Commission deny authorisation for the proposed direct connection between the United States and Hong Kong within the Pacific Light Cable Network. Despite the commercial rationale supporting the project, the committee argued that the connection could expose American communications to access by Chinese authorities. This reasoning reflects a conception of security centred on the political jurisdiction of landing points, comparable in certain respects to the principles that had informed British imperial cable policy. Similar considerations can be identified in contemporary American strategic debate, where the All-Red Line has explicitly been proposed as a historical model for securing fibre-optic networks. NATO's surveillance activities in the Baltic Sea and European Union initiatives concerning publicly funded cable repair capabilities likewise reflect the growing involvement of states and international organisations in the security of submarine infrastructure.

An important difference from earlier periods, however concerns the changing structure of ownership. An increasing proportion of new submarine cables is financed by a small number of large digital platform companies. Google, Meta, Microsoft and Amazon are now involved in more than sixty cable systems, compared with approximately twenty in 2017. The growing strategic and political relevance attributed to these networks therefore coexists with a system in which substantial infrastructural assets are privately owned and operated.

The renewed attention to submarine cable security may fade as other international developments come to dominate political and public debate. Nonetheless, a longer historical perspective suggests that the relative depoliticisation of these infrastructures during the 1990s constituted an exceptional period rather than a permanent transformation. Throughout most of their history, submarine communication networks have been shaped by political considerations concerning the location of routes, control over landing points, dependence on foreign territories and the capacity to interrupt an adversary's communications. Their geographical configuration has consequently remained closely connected to questions of power and strategic vulnerability, and the renewed political attention directed towards these infrastructures clearly reflects the reassertion of their longstanding geopolitical significance.

Edoardo Maria Landoni *is a Research Fellow affiliated with the Violence & Security Program at T.wai and Teaching Assistant at the University of Milan and at the University of Pavia. His research focuses on geopolitics and strategic studies, with particular attention to how information and communication technologies reshape power, security, and international competition.*