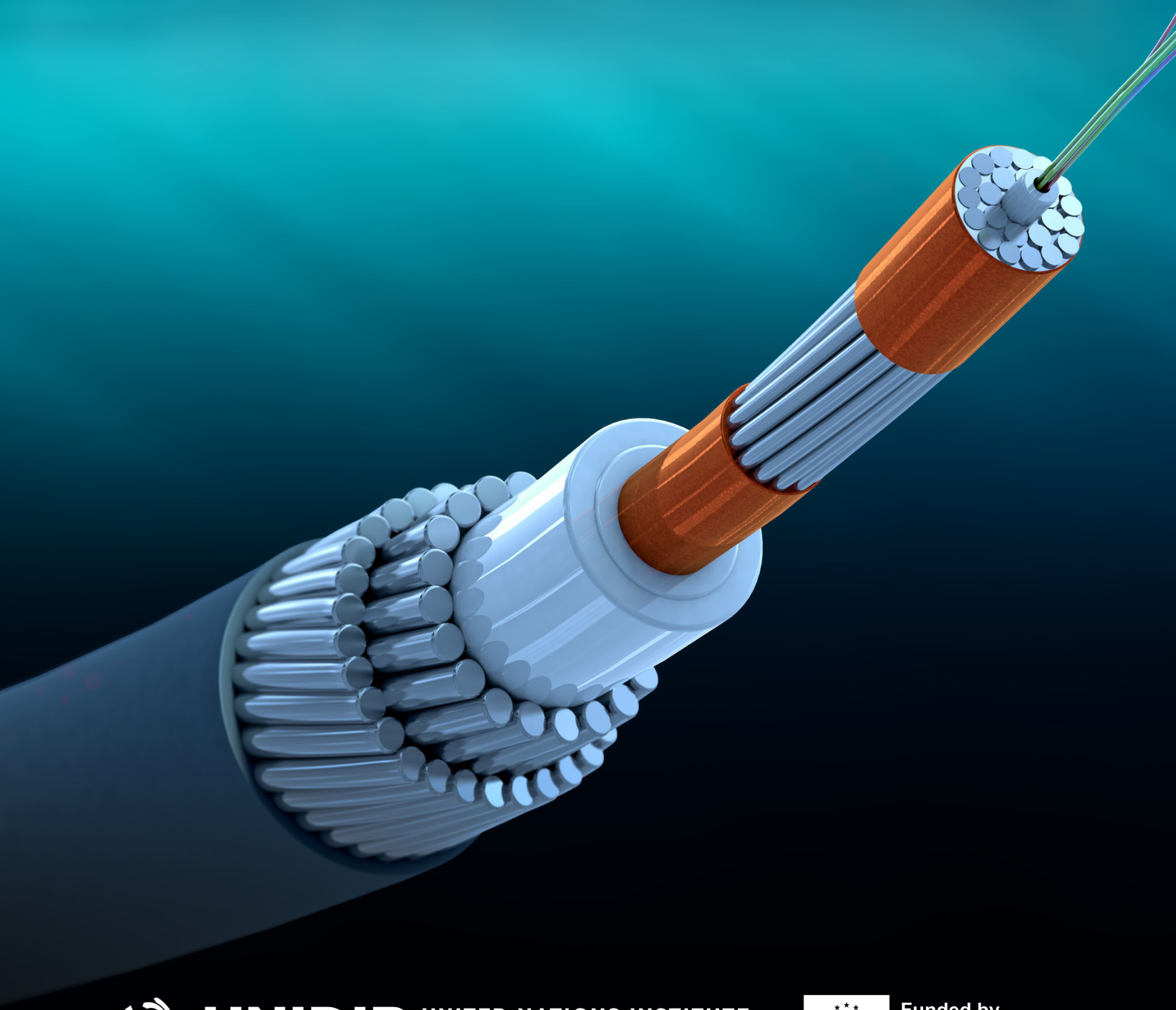
WADING MURKY WATERS

Subsea Communications Cables And Responsible State Behaviour

CAMINO KAVANAGH



UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Funded by the European Union

ACKNOWLEDGEMENTS

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This publication was funded by the European Union as part of UNIDIR's Security and Technology Programme, which is supported by the governments of Czechia, Germany, Italy, the Netherlands, Switzerland, and by Microsoft. The author extends her thanks to the diverse body of experts from across industry, government and academia that provided substantive feedback on different iterations and sections of this paper.

Design and layout by Trifecta Content Studio.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

CITATION

C. Kavanagh. Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour. Geneva, Switzerland: UNIDIR, 2023.

NOTE

CONTENTS

ABOUT THE SECURITY AND TECHNOLOGY PROGRAMME

Contemporary developments in science and technology present new opportunities as well as challenges to international security and disarmament. UNIDIR's Security and Technology Programme (SecTec) seeks to build knowledge and awareness on the international security implications and risks of specific technological innovations and convenes stakeholders to explore ideas and develop new thinking on ways to address them.

ABOUT THE AUTHOR

Dr. Camino Kavanagh is Visiting Senior Fellow at King's College London and Non-resident Scholar at the Carnegie Endowment for International Peace. She also works as an international consultant on issues pertaining to cyber, emerging technologies, international security and conflict. Camino served as Advisor to the Chairs of the 2019-2021 Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE) on ICTs and International Security and Rapporteur/Consultant to the 2016–2017 GGE on the same topic.

ABBREVIATIONS AND ACRONYMS

GGE	Group of Governmental Experts
ICPC	International Cable Protection Committee
ICT	Information and communications technology
OEWG	Open-ended Working Group
UNCLOS	United Nations Convention on the Law of the Sea

EXECUTIVE SUMMARY

This report is about subsea communications cables. These cables are an essential element of the information and communications technology (ICT) ecosystem, transmitting practically all our telecommunications and data. Their security and resilience are critical to the well-being and functioning of societies across the globe, and to international security and stability. Technological advances are enabling the transmission of data through subsea communications cables at speeds that could hardly have been envisaged some 150 years ago when the first cables were laid on the seabed. They are enabling connectivity between historically remote or abandoned countries and regions and the rest of the world, which combined with other efforts will hopefully unleash much-needed social and economic dividends. And they are enabling scientific research, including that essential to understanding the environmental changes affecting our planet. However, the global network of subsea communications cables and the data transmitted through them are at risk.

This report suggests that there is an urgent need to accelerate efforts to strengthen the resilience of this vital infrastructure and its physical, network and data layers. It fully notes the nature of State-backed activity that can affect the cables on the seabed, on land or via cyberspace, and the thrust of many policy decisions shaping subsea cable investment and routing decisions. It recognizes that individual States and certain regions or subregions have legitimate concerns regarding the security of subsea communications cable systems, especially in the current environment of heightened geopolitical tensions and technological competition. It nonetheless questions the direction of current responses, arguing that, to avoid the mistakes of the past, a cooperative approach anchored in strengthening the resilience of the systems globally is also required. Its recommendations are directed mainly at States, although it recognizes the importance of the private sector, academia and the technical community to such efforts. It draws from existing recommendations and commitments, including those of the International Cable Protection Committee and United Nations Member States working under the auspices of the General Assembly's First Committee on Disarmament and International Security on ICTs and international security. The recommendations are organized under three thematic areas: (1) subsea communications cables as critical infrastructure; (2) enhanced public–private cooperation; and (3) a more comprehensive and principles-based policy agenda. It is hoped they serve as a basis for advancing ongoing discussions on responsible State behaviour in this area.

INTRODUCTION

Just over a decade ago, as the third Group of Governmental Experts (GGE) on information and communications technology (ICT) and international security was concluding its work, a number of academic reports on subsea communications cables were published.[1] They shed light on emerging risks to subsea cable systems and also highlighted many of the gaps in the international subsea cable legal regime and broader governance challenges. Back then, only two hundred or so subsea cables were operational, and largely owned and operated by telecommunications carriers. Today, the number of cables in operation has doubled and technological advances in the field of photonics are guaranteeing once unimaginable speeds and capacity. The nature of the industry has dramatically changed, along with new risks to the cable systems. And all of this while our dependency on the cables and the broader ICT ecosystem continues to increase. While threats relating to subsea communications cables rarely received much attention in cyber policy circles, this is now changing.

In March 2022, in the context of the current 2021–2025 Open-ended Working Group (OEWG) on security of and in the use of ICTs, a representative from a small yet geostrategically located State referenced subsea cables in their remarks. The aim was to bring attention to the resources and capacities required to protect the undersea cables passing through the State's waters, and the challenges it faces in ensuring the reliability and availability of such critical communication links for a range of countries across the Horn of Africa, South Asia and Europe, particularly in light of growing geopolitical tensions. During the same meeting, another representative cautioned that despite internationally recognized norms of behaviour relevant to ICTs, some States were targeting critical infrastructure such as subsea communications cables, with potentially significant disruptive effects.[2]

These brief yet important references to subsea communications cables, their vulnerability to attack, and related resiliency and capacity issues during a session of the OEWG were a small indication of growing State concerns about the threats emerging around this most critical of information infrastructures.[3] Yet they went largely unheeded. Then, several months later, the Nord Stream explosions shifted the attention of States downwards, to the

[1]See, for instance, Douglas R. Burnett, et al. (eds) (2013), Submarine Cables: The Handbook of Law and Policy, BRILL; Michael Sechrist (2012), "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems", Harvard Kennedy School; and Michael Sechrist (2010), "Cyberspace in Deep Water: Protecting Undersea Communications Cables by Creating an International Public–Private Partnership", Harvard Kennedy School.

[2]See remarks by representatives of Djibouti and the United States, Open-ended Working Group second substantive session, https://meetings.unoda.org/meeting/57871/statements?f%5B0%5D=segment_statements_%3ASecond%20substantive%20session&f%5B1%5D=segment_statements_%3AThird%20substantive%20session.

[3]The topic had been raised before by the government of Singapore in the context of the United Nations and its work on ICTs and international security, but for a range of reasons did not gain much traction within this particular forum.

cable systems it hosts, and to the enormity of our collective dependency on them. The situation suggested a need for greater information-sharing among relevant industry and government actors, and, perhaps, new measures to strengthen their resilience.[4]

It is not clear, though, whether diplomats are prepared for such a conversation. Despite subsea cables' long and winding history, the policy and research communities have been critiqued for not having much understanding of "how [the global network of cables] operates, how it is regulated, who controls it, and how it is protected from vulnerabilities".[5] On the policy side, there is likely much strategic ambiguity regarding what some policymakers, or the private interests that own and operate the majority of subsea communications cable systems, want to reveal or can publicly discuss. But the dearth of awareness and understanding in many policy circles remains strong. On the research side, the body of literature on subsea cable-related issues has grown significantly, with approaches from a range of perspectives: science and technology, engineering, maritime security, public international law, environmental protection, governance and security studies, history, and archaeology to name but a few.[6] And much-needed, interdisciplinary research is also emerging.[7] Nonetheless, recent developments suggest that the time is ripening for a more in-depth conversation on subsea communications cables, on the adequateness of the existing cable governance regime, and what might be done to strengthen it. Such conversations are already commencing at regional and national levels.[8] This report is an attempt to provide a basis for a more global and inclusive conversation, anchoring it firmly within ongoing multilateral discussions.

This report approaches subsea communications cables from a systemic perspective: as core elements of the broader ICT ecosystem. It begins with an overview of developments in subsea cable technology and associated 'wet' (undersea) and 'dry' (land) plant infrastructure and the main actors involved in the subsea cable industry.[9] It then provides an overview of the more commonly cited threats and vulnerabilities relevant to subsea cable systems and related infrastructure, followed by an introduction to the extant subsea cable governance regime. Drawing in part from the Government Best Practices of the International Cable

---

[4]See, for instance, the section "Future Secure Connectivity Projects" in the US–EU Joint Statement of the Trade and Technology Council of 5 December 2022.

[5]Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", Contemporary Security Policy 42:3, p. 392.

[6]Ibid.

[7]See, for example, Christian Bueger and Tobias Liebetrau (2022), "Security Threats to Undersea Communications Cables and Infrastructure—Consequences for the EU", https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf.

[8]Ibid.

[9]The 'wet plant' is the segment of the cable running from one beach manhole on one landmass to another. It includes the fibre-optic cable, repeaters, equalizers and branching units. The 'dry plant' is traditionally the terrestrial segment of an undersea cable system, running from the beach manhole to the cable landing station, usually located a few hundred metres from the beach manhole and connected by a short, repeater-less fibre link, although this configuration is changing as cable system architectures develop.

Protection Committee[10] and existing recommendations negotiated under the umbrella of the General Assembly's First Committee,[11] it concludes with some preliminary recommendations on cooperative steps that governments can take to advance responsible State behaviour and to strengthen the resilience of subsea cable systems and related infrastructure. These recommendations are organized around three thematic areas: subsea communications cables as critical infrastructure; public–private collaboration; and a more comprehensive and principles-based policy agenda.

[10]In 2022, following significant consultations, the International Cable Protection Committee published its Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables to "assist governments in developing laws, policies, and practices to foster the development and protection of submarine telecommunications cables, the infrastructure of the Internet"; see https://www.iscpc.org/publications/icpc-best-practices/.

[11]Since 1998, United Nations Member States working under the auspices of the General Assembly's First Committee on Disarmament and International Security have been engaged in discussions on ICTs and international security. Over time, a series of Groups of Governmental Experts (GGE) and an Open-ended Working Group (OEWG) have recommended a series of measures relevant to the responsible behaviour of States in their use of ICTs. These include three norms specifically focused on critical infrastructure. In 2021, the sixth GGE and the first OEWG involving all 193 Member States advanced the discussion on these norms, noting that the critical infrastructure referred to in the relevant recommendations can include those infrastructures essential to the general integrity or availability of the Internet. This report assumes that the latter includes subsea communications cables and associated land infrastructure, components and systems that facilitate the transmission of data

What's in a Modern Subsea Communications Cable?

The first subsea cables were laid in the nineteenth Century, first between Britain and France, and then traversing the Atlantic between Valentia Island in Ireland and Heart's Content in Newfoundland. [12] In these systems, electrical signals were transmitted over a wire laid between two telegraph stations. Morse code was used to assign a set of dots and dashes to each letter of the English alphabet, allowing for the simple transmission of complex messages. The speed with which messages could be delivered was ground-breaking, and the new technology deemed "far more useful to mankind than was ever won by conqueror on the field of battle" with the potential of serving as a "bond of perpetual peace and friendship" between nations.[13]

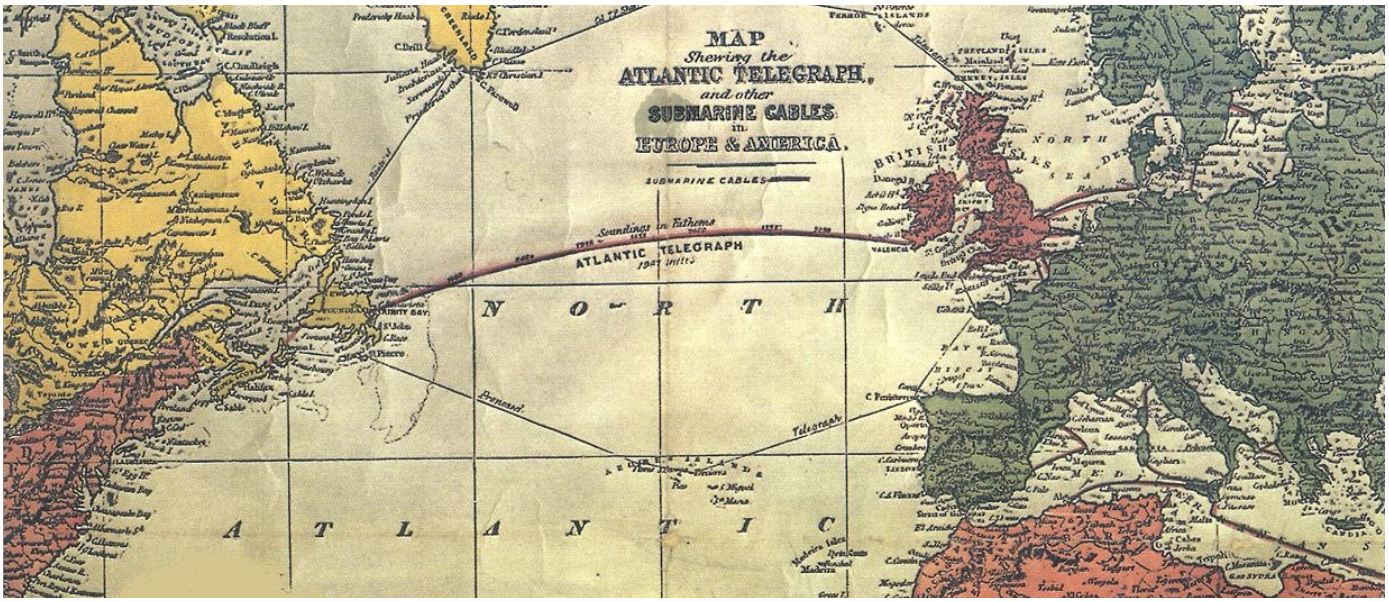


Figure 1. Map of the 1858 Transatlantic Telegraph Cable

Despite their spread across the world's oceans during those initial decades, telegraph cables fell out of use in the early twentieth century, superseded by other emerging technologies such as the telephone and later, the fax. Further advances in communications technology led to the laying of the first transatlantic telephone cable system in the 1950s, followed three decades later by the first transatlantic fibre-optic cable system. Thirty-five years have since passed and some 530 cable systems are currently active or under construction.[14] Subsea fibre-optic cables are now the backbone of our communications infrastructure: more than 95 per cent of global Internet, voice and data traffic passes through this vast

[12] To commemorate this significant moment in global communications history, Ireland and Canada are jointly seeking UNESCO World Heritage status for the transatlantic telegraph stations in Valentia and Heart's Content; see https://www.irishtimes.com/ireland/2022/07/22/valentia-islands-transatlantic-cable-to-be-put-forward-for-unesco-world-heritage-status/.

[13] Words of US President James Buchanan in his congratulatory message to Queen Victoria, the first exchanges over the trans-Atlantic telegraph in 1858. The first trans-Atlantic message took 17 hours to send, at 2 minutes and 5 seconds per letter.

[14] TeleGeography, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

submerged network. Literally all our private, business and military communications depend on it, as do global financial transactions and many defence systems. The strategic value of the infrastructure continues to grow in tandem with our digital dependence, the advent of 5G and the high-quality, low-latency connectivity needs of economic centres, and the commercial and strategic value inherent in access to new markets and the data that is hosted or that can be accessed therein.[15]

Today's subsea cables use optical fibre technology to transmit data. Some individual cable systems can be as long as 45,000 kilometres.[16] Together they represent approximately 1.3 million kilometres of in-service cable across the globe. The cables are made up of multiple pairs of optical fibres, roughly the diameter of a human hair, which are then covered in

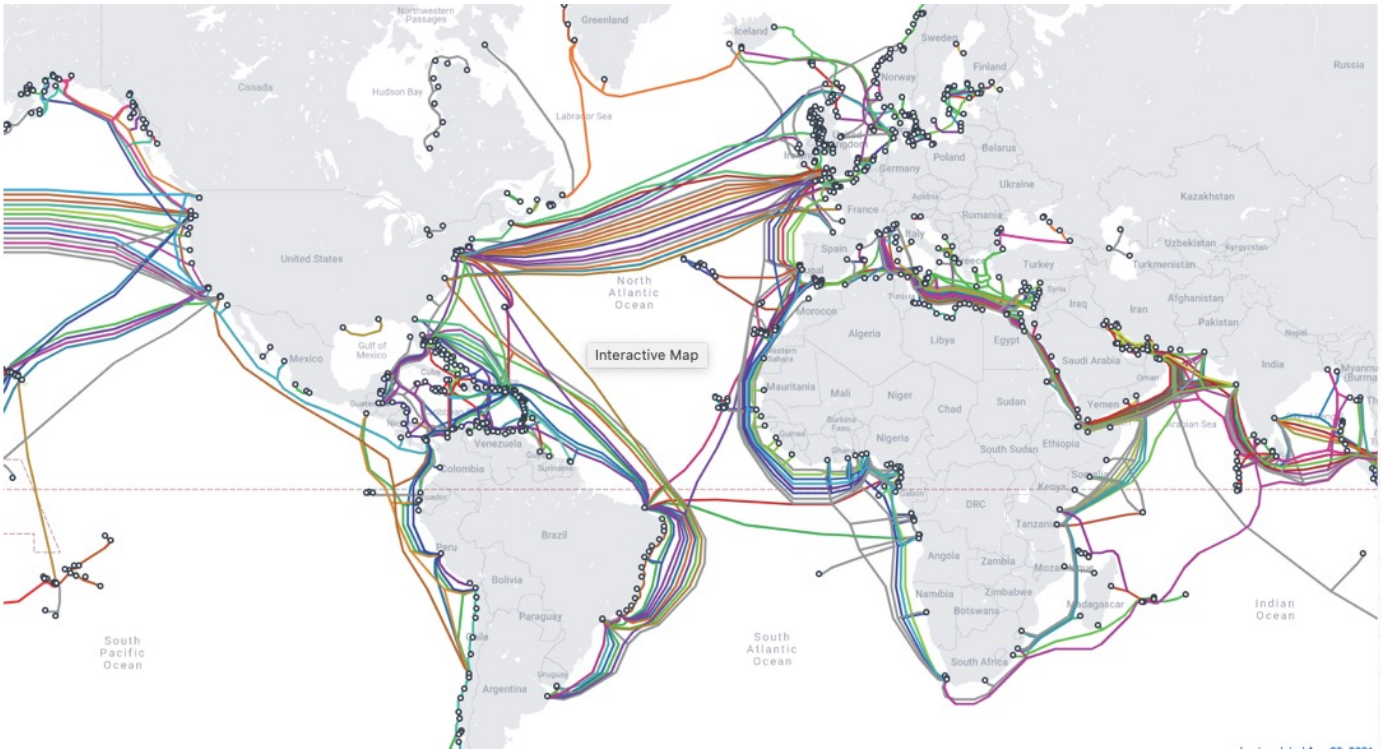


Figure 2. Submarine Cable Map 2022[17]

silicone gel, and sheathed in varying layers of plastic, steel wiring and copper. Sometimes additional layers of steel wire are applied to the outside of the cable to armour it against external damage. The thickness of steel armouring is generally determined by sea depth

[15] Hilary McGeachy (2022), "The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns", Australian Journal of International Affairs 76:2.

[16] DataCenterDynamics (2022), 'World's Longest Subsea Cable Lands in Djibouti, East Africa', https://www.datacenterdynamics.com/en/news/worlds-longest-subsea-cable-lands-in-djibouti-east-africa; Reuters (2022), "MTN Lands Subsea Cable in South Africa to Boost Africa's Connectivity", https://www.reuters.com/world/africa/mtn-lands-subsea-cable-south-africa-boost-africas-connectivity-2022-12-13/.

[17] TeleGeography's 2022 Submarine Cable Map depicting 486 cable systems and 1,306 landings currently active of under construction; see https://submarine-cable-map-2022.telegeography.com/.

and proximity to commercial marine activity. In shallow water (usually defined as less than 1000 m), the cable may also be buried under the seabed to provide further protection from, for instance, ships' anchors and fishing operations.

Until just over a decade ago, intensity modulated direct detection was the optical transmission technology most commonly used in subsea cables. This method transmits information over subsea and terrestrial optical fibres by using laser pulses to encode digital data. Since then, further advances in coherent optical transmission have allowed single-channel data rates to increase more than a hundred fold.[18] In addition, wavelength division multiplexing has increased the number of channels carried per fibre.[19] Cable capacities vary depending on the cable system, but advances such as spatial division multiplexing will allow newer systems to carry as much as 500 terabytes per second.[20] In systems longer than a few hundred kilometres, optical amplifiers (housed in watertight containers known as repeaters) boost the signals along the length of the cable roughly every 100 km.

Traditional cable builds reach land within one of the 1,306 cable landing stations currently in operation across the globe, from where the data is then routed to connect to terrestrial systems.[21] Under a traditional station-to-station system, the stations house the 'dry plant' infrastructure, which includes the submarine line terminal equipment that controls its operations, and the equipment that powers the cable. This traditional architecture has shifted in recent years, pushing greater convergence between subsea and terrestrial fibre networks and data centres. For instance, in a system connecting data centres, the power equipment may be housed at a smaller modular landing station near the shore, and the terminal equipment inland at a data centre or "or a connectivity-rich, carrier-neutral interconnection colocation facility".[22] Such so-called 'open cable' systems separate the terminal equipment from the 'wet plant' and allow for system upgrades and equipment diversification, including in legacy systems. The type of system will ultimately depend on the interests of the end users in terms of the capacity they are purchasing (access to major markets, endpoints, Tier 1 IP networks, Internet exchange points, redundancy options, connection to cloud aggregation services, etc.), although a final decision will be contingent on a range of factors including whether it is a joint build (i.e., commissioned by two or more purchasers), as well as market openness, cost, distance, geographical conditions, the regulatory environment including national foreign investment regulation, and so forth.[23] New ecosystems are likely to continue emerging in the coming period.

[18] See Ciena, "What Are Coherent Optics", https://www.ciena.com/insights/what-is/What-Is-Coherent-Optics.html; and Google (2022), "Google's Subsea Fiber Optics, Explained", https://cloud.google.com/blog/topics/developers-practitioners/googles-subsea-fiber-optics-explained.

[19] Ibid.

[20] Greater capacity can be realized through spatial division multiplexing in which more fibre pairs carry channels with lower power and signal-to-noise ratio; see https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

[21] Ibid.

[22] Vinay Nagpal (2019), "Convergence of Data Centers, Subsea and Terrestrial Fiber", Pacific Telecommunications Council.

[23] Ibid.

Implementing a new cable project can take anywhere between 2.5 to 5 years from initial planning to system commissioning. Like any infrastructure project, it involves a number of steps and lengthy negotiations.[24] Once an agreement is reached, building commences. This involves installing the 'wet' (submerged) plant and 'dry' (land) plant infrastructure, as well as the network management and monitoring infrastructure necessary for the subsea cable system to work reliably.[25] The design life cycle of a cable system is approximately 25 years, although many can extend beyond that timeframe if revenues continue to exceed costs.[26] Currently, a significant number of cables are reaching their end of life.

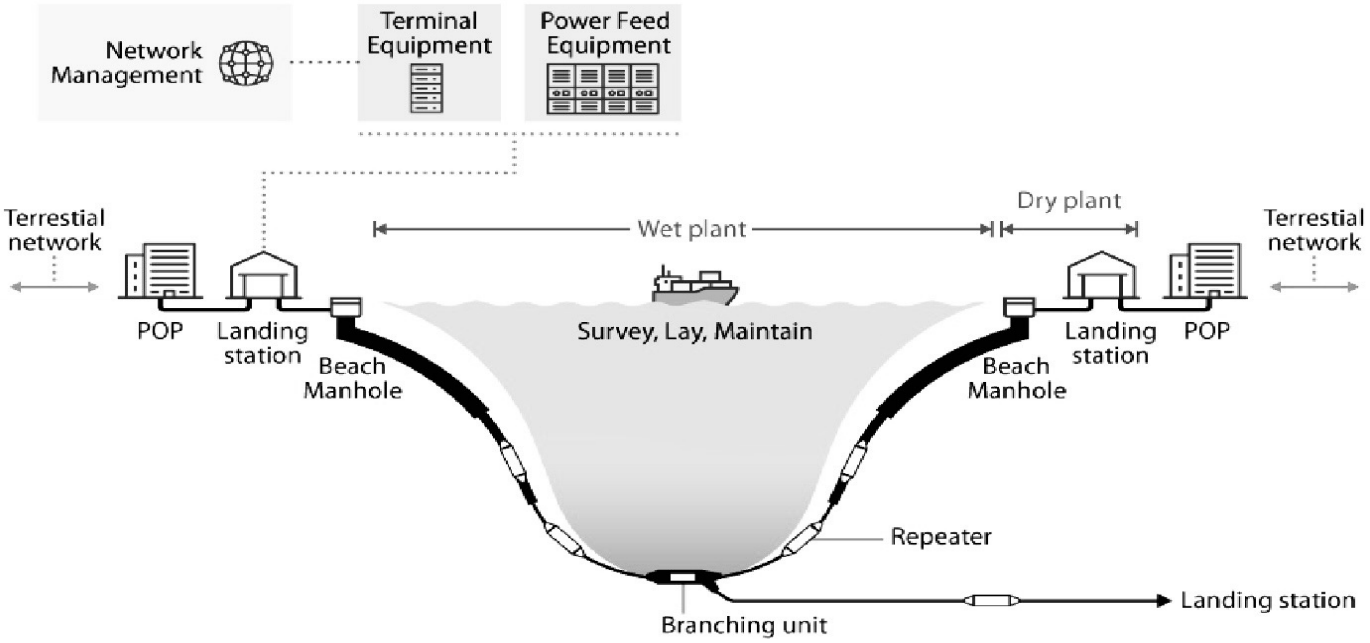


Figure 3. Subsea Cable Systems—Wet and Dry Plant Infrastructure and Components[27]

In principle, risk management and mitigation are integrated into the cable system design and network management process to offset the potential risk of system downtime and associated repair costs, and to ensure the highest degree of resilience. [28] For one, the architecture of the cable systems ensures that a deliberate degree of redundant capacity

[24] For instance, the supply contract alone typically consists of six main parts, including the terms and conditions of contract; technical specifications of the project; a pricing schedule; a plan of work; a billing schedule; and the supplier's system description. Often these contractual arrangements need to be negotiated with a range of actors, since cable projects are traditionally implemented through consortia or as joint builds.

[25] See footnote 9.

[26] To offset the negative effect of lower capacity prices on revenues, cables need to continually add capacity; see Alan Maudlin (2018), "The Next Mass Extinction: Ageing Submarine Cables", https://www2.telegeography.com/submarine-networks-world-2018.

[27] Jill C. Gallagher (2022), "Undersea Telecommunication Cables: Technology Overview and Issues for Congress", US Congressional Research Service, p. 5, https://crsreports.congress.gov/product/pdf/R/R47237.

[28] According to Subcom, an undersea cable repair can cost in excess of US$ 1 million and typically takes 2 weeks to return the cable to service—or more, depending on permitting requirements, weather, and other factors. Regarding cybersecurity threats, connectivity providers need to be able to protect the traffic they enable through built-in security features. These may include a next-generation firewall (NGFW), secure remote access, and unified threat management (UTM) services. Moreover, connectivity that offers end-to-end encryption, network security, and application level filtering allow for greater quality of service and can prevent cyber security threats; see Brendan Press (2021), "The Role of Subsea Cables in a World Going Local', https://datacentremagazine.com/automation/role-subsea-cables-world-going-local.

is built into the systems. This means that damage to a cable should generally not have second- or third-order effects on services or infrastructure. It is expected that resiliency will be further advanced as new capacity is added to current systems. In the past, most attention was paid to risks associated with the physical infrastructure and components of cable systems, mainly from faults and damage caused by commercial maritime activity.

Today, that focus has broadened to cover risks that might emerge on the data and network layers of the systems. The latter include fibre and cybersecurity risks that may emerge during the manufacturing process or at vulnerable points such as submersed hardware components, beach manholes, cable landing stations, 'points of presence' or interconnection facilities, Internet exchange points and data centres, as well as on cable network management systems, which run on software and tend to be remotely operated.[29] Related risk management approaches include hardening the physical security of relevant buildings, including through strengthened peripheral security as well as innovations in modular cable landing station builds, and applying cybersecurity geomesh architectures, strong data encryption and other zero-trust security controls and technologies across core elements.[30] Advances in cable system architectures can also contribute to greater resilience as newer shared systems reportedly limit access to physical and virtual elements of a cable at the terminal equipment.[31] Likewise, there are standards and techniques that can help both to prevent and detect vulnerabilities in the optical hardware and potential interference with or attacks on the optical networks. For instance, sensing techniques such as optical interferometry and distributed acoustic sensing in cables are increasingly applied to monitor near-shore segments of a cable in order to detect nearby activity or irregularities and faults in cable transmission.[32] More recent advances in sensing techniques continue to emerge on other parts of the system, sending promising signs for network integrity as well as environmental monitoring.[33]

---

[29]Michael Sechrist (2012), "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems", Harvard Kennedy School; see also Nadia Schadlow and Brayden Helwig (2020), "Protecting Undersea Cables Must be Made a National Security Priority", Defense One, https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/; and Olga Khazan (2013), "The Creepy, Long-Standing Practice of Undersea Cable Tapping", The Atlantic, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

[30]The core elements referred to are identity, endpoints, data, apps, infrastructure and networks; see Microsoft (2022), "Guiding Principles of Zero Trust", https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview.

[31]Communication with industry representative, December 2022.

[32]Unlike earlier remote supervisory functions which were conducted through hardware placed on each end of the cable, in new cable systems the fibre itself is the sensor. For more on DAS, see SAGE, "Distributed Acoustic Sensing (DAS) Research Coordination Network (RCN)", https://www.iris.edu/hq/initiatives/das_rcn.

[33]New research has also demonstrated "the first real-time coherent transceiver with built-in real time phase and polarization sensing while simultaneously transmitting information". The researchers report having "successfully transmitted over 12,800 km while continuously performing environmental sensing"; see M. Mazur et al. (2022), "Transoceanic Phase and Polarization Fiber Sensing using Real-Time Coherent Transceiver", Optical Fiber Communications Conference (OFC) 2022, pp. 1–3, https://opg.optica.org/abstract.cfm?uri=OFC-2022-M2F.2. Regarding related developments on terrestrial systems, see Optica (2023), "Scientists Perform Real-Time Environmental Sensing over 524 Kilometers of Live Aerial Fiber", https://phys.org/news/2023-01-scientists-real-time-environmental-kilometers-aerial.html.

Subsea fibre-optic communications cables are largely owned and operated by private enterprise. Traditionally, the main owners and operators were telecommunications carriers that used the model of a consortium to work with parties interested in using the cable and to offset costs. In the boom-and-bust decade of the 1990s, a number of private companies invested in subsea cables, yielding a profit by selling off capacity to telecom companies and other private actors.[34] Both financing models exist today, yet there are significant new developments in terms of geographical spread and the type of private entities involved. For instance, the past decade has seen Chinese companies play an ever-growing role in subsea cable project investments across the world, often as part of consortiums, and regionally in cable maintenance and repair.[35] These investments are coupled at home with research and development and manufacturing investments in ultra-high-speed and -capacity optical transmission and related subsea cable and networking technologies.[36] The industry has also witnessed the arrival of major cloud service providers and hyperscalers such as Meta, Alphabet, Microsoft, and Amazon. In their drive to connect new, large-scale data centres and cloud networks, these global behemoths have added capacity "at a compound annual rate of at least 70 percent between 2015 and 2019 across six of the world's seven regions",[37] changing traditional cable investment and ownership structures in many of these same regions, and "surpass[ing] internet backbone providers to become the leading owners of subsea cable capacity".[38] The number of independent subsea cable infrastructure developers that own and operate cable systems has also increased. Drawing lessons from the challenges of other ownership structures, they have reportedly created an unexpected differentiation in the market.[39] Together, these are the most visible actors in the industry. Behind the scenes a plethora of specialized private companies and technical bodies provide services that stretch across the life cycle of a cable system.

---

[34]The 'bust' years refers to the fact that many of these companies subsequently went bankrupt when the internet industry imploded and capacity was no longer required.

[35]For instance, Chinese company HMN Technologies (formerly Huawei Marine) was involved in 13 different cables projects between 2012 and 2019, most of them outside its home region; Lane Burdette (2021), "Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy", Journal of Public and International Affairs, https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy. See also Hilary McGeachy (2022), "The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns", Australian Journal of International Affairs 76:2; Jonathan E. Hillman (2021), "Securing the Subsea Network: A Primer for Policymakers", Centre for Strategic and International Studies; and Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", Contemporary Security Policy 42:3. Chinese company involvement in cable builds has since decreased for a number of reasons, some of them driven by the national security concerns of other States. Chinese maintenance and repair company SBSS is predominantly active in Asia, and services both the fibre-optic and power cable sectors.

[36]Notice of the State Council on the Publication of Made in China 2025 (2015) No. 28, PRC State Council, p. 19, 'New Generation IT Industry'. Translation made available by Center for Security and Emerging Technology , 10 March 2022, https://cset.georgetown.edu/publication/notice-of-the-state-council-on-the-publication-of-made-in-china-2025/

[37]Matthew P. Goodman and Matthew Wayland (2022), "Securing Asia's Subsea Network: U.S. Interests and Strategic Options", CSIS Briefs, p. 3.

[38]Ibid. See also Alan Mauldin (2017), "A Complete List of Content Providers' Submarine Cable Holdings", https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list.

[39]Suvesh Chattopadhyaya (2018), "A New Coming for Submarine Cable Systems—the Independent Infrastructure Developers", https://www.submarinenetworks.com/en/insights/a-new-coming-for-submarine-cable-systems-the-independent-infrastructure-developers ; Olivier Pinaud (2023), "Big Tech Colonizes Seabed to Assert Control of the Internet", Le Monde, https://www.lemonde.fr/en/international/article/2023/01/02/big-tech-colonizes-seabed-to-assert-control-of-the-internet_6010073_4.html.

Government ministries and agencies, too, play a strong hand in the governance and protection of subsea cables, their regulatory and policy roles extending across the life cycle of a cable system and its subsea and land infrastructure. These have traditionally included ministries, departments, and agencies responsible for telecommunications, maritime and shipping affairs, fisheries, the environment, customs, law enforcement and defence. Today, they also include ministries and agencies responsible for cybersecurity and critical infrastructure protection, digital transformation, foreign policy, innovation, trade, investment, and development.[40] Regional organizations such as the Asia–Pacific Economic Cooperation (APEC) forum, the Association of Southeast Asian Nations (ASEAN) and various European Union bodies produce policy, research and guidance relevant to subsea communications cables.[41] Specialized international bodies, too, play a role, for instance the International Telecommunication Union (on technical standards), the International Hydrographic Organization (on charting and spatial separation issues), the United Nations Office on Drugs and Crime (on maritime security-related technical assistance and capacity-building issues, including with regard to subsea cable protection), and the Intergovernmental Conference on Marine Biodiversity of Areas Beyond National Jurisdiction (relevant to resolution 72/249 on the sustainable use of marine biological diversity of areas beyond national jurisdiction) which just agreed a new international legally binding instrument.[42] As well, a number of non-governmental organizations, technical bodies and research institutes play an important role.[43]

[40] ICPC (2022), "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables", https://www.iscpc.org/documents/?id=3733.

[41] See for instance, APEC publications, including those stemming from its Supply Chain Connectivity Framework Action Plan; ASEAN's Digital Masterplan 2025, and its 2019 Guidelines for Strengthening Resilience and Repair of Submarine Cables; Directive (EU) 2022/2555 of 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555; see also Christian Bueger and Tobias Liebetrau (2022), "Security Threats to Undersea Communications Cables and Infrastructure—Consequences for the EU", https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf.

[42] Statement of the UN Secretary-General at the Inter-Governmental Conference on a legally binding instrument under the United National Convention on the Law of the Sea (UNCLOS) on the conservation and sustainable use of marine biological diversity of areas beyond national jurisdiction, 05 March 2023, https://www.un.org/bbnj/sites/www.un.org.bbnj/files/sgstatementbbnj5resumed.pdf. See also https://www.un.org/bbnj/.

[43] The list is long, but some key organizations include Safe Seas on maritime issues, and the Institute of Electrical and Electronics Engineers and the Internet Society on technology and network/cyber issues.

Threats and Vulnerabilities

In comparison to the copper cables of the nineteenth century, today's fibre-optic cables are highly reliable, engineered to what is known as the '5 nines standard' in that they are available 99.999 per cent of the time and "suffer few major disruptions in proportion to their heavy dispersion throughout the world".[44] Nonetheless, faults do occur, estimated at approximately 200 per year.[45] As discussed further below, when faults and disruptions do occur, the effects can be significant, particularly when automatic rerouting to unused and available capacity on other subsea cables and terrestrial or satellite networks is not possible.

The threats to subsea cable communications systems are multidomain, spread across sea, land and cyberspace. They can be linked to natural phenomena or human activity (unintentional or intentional), affecting the cables themselves and the transmission of data or other parts of the infrastructure, including the amplifiers, landing stations, maintenance and repair ships, network management systems and cable supply chains.[46] The cables also tend to be highly concentrated geographically at sea and on land at so-called 'choke points', which makes laying and repair of the cables difficult in normal circumstances, and easy to block in situations of tension or crisis.[47]

The cables themselves are vulnerable to natural phenomena related to weather (storm surges, typhoons, hurricanes), geology (earthquakes, fault lines, undersea landslides, volcanic eruptions) and the sea environment (current density, waves). Disruptions caused by natural phenomena tend to take place closer to land, affecting several cables at the same time, and redundancy is lost. Such events are even more problematic when a country is serviced by just one cable. Take, for example, the underwater volcanic eruption near Tonga and ensuing tsunami on 15 January 2022, which severed the sole subsea cable connecting Tonga to the rest of the world via Fiji. While low-grade connectivity was assured via satellite links a week after the event, it nonetheless took over five weeks to repair the cable and to restore full connectivity to the main island of Tongatapu, and several months to repair the domestic cable connecting the main island with outlying islands that were worst hit by the tsunami.[48]

---

[44]Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", Contemporary Security Policy 42:3, p. 396.

[45]Per discussions at the 2019 ICPC plenary, the fault rate per 1,000 km was static or slightly decreasing over the last decade, despite the growth in the total length of cables in service.

[46]For instance, according to Quintillion, growing demand and phenomenon such as Covid have led to shortages in fibre cable and ODN infrastructure and in electronic components such as flash memory, capacitators and semiconductors. Quintillion, "Connecting the World to Fiber: The Subsea Cable Industry's 5 Biggest Challenges", November 26, 2021, https://www.quintillionglobal.com/connecting-the-world-to-fiber-the-subsea-cable-industrys-5-biggest-challenges/

[47]See, for instance, Matt Burgess (2022), "The Most Vulnerable Place on the Internet", https://www.wired.com/story/submarine-internet-cables-egypt/, which discusses the vulnerability of the Red Sea route as "one of the world's largest internet chokepoints".

[48]Simon Scarr et al. (2022), "The Race to Reconnect Tonga", Reuters, https://www.reuters.com/graphics/TONGA-VOLCANO/znpnejbjovl/.

Cable failures or disruptions can also be caused by commercial marine activity such as fishing and anchoring. According to ICPC statistics , disruption by fishing and anchoring tend to be the most common form of disruption, representing approximately 70 per cent of most cable failures.[49] Other kinds of commercial activity that can cause cable disruptions include shipping, dredging, as well as deep-sea mining, which is intensifying in some maritime regions.

Sometimes market dynamics can also be behind cable failures. This can occur if owners try to lower the cost of cable builds by using lower quality equipment and components in the construction of a cable system.[50] Efforts to increase efficiency can also be problematic. For instance, the move to remote network management systems drew attention due to the vulnerability to exploitation of the systems' software, although these remote systems have been significantly hardened in line with the increase in attention paid to cybersecurity-related risks over the past decade.[51] There is also concern that an ever more complex digital ecosystem, with layered and tiered dependencies operating at a global scale may trigger a series of tiered failures not currently considered in current risk management and mitigation frameworks.[52]

Beyond cable faults per se, supply chain issues such as shortages in or dependencies on core components can pose important risks, particularly when urgent repairs are needed.[53] So, too, can limited investment in maintenance and repair shipping capabilities and in responding to skilled workforce shortages, both of major concern to the industry at present.[54]

While not commonly discussed, poorly crafted government policy and regulatory frameworks "can also exacerbate risks of damage and reduce resilience" of the cable systems, and delay repair activity[55], as can a lack of clarity regarding the roles and responsibilities of national authorities. For many in the industry, national security-guided decisions regarding cable routing and investment can also undermine the competitiveness of industry actors and stymie innovation. They can also produce new security risks.

---

[49]ICPC (2022), "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables" Section 2, "Fishing and anchoring risks", https://www.iscpc.org/publications/icpc-best-practices/

[50]Communication with cable industry representative, 2 December 2022.

[51]Michael Sechrist (2012), "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems", Harvard Kennedy School.

[52]Communication with national cybersecurity centre director, 24 January 2022.

[53]On supply chain issues, particularly component supply (including semiconductors), see Jim Fagan, "Managing tight supply chains in global subsea connectivity", Mission Critical, 25 October 2022, https://www.missioncriticalmagazine.com/articles/94311-managing-tight-supply-chains-in-global-subsea-connectivity; Sebastian Moss," Global Global shortage of fibre optic cables leads to delays, price increases", DataCenterDynamics,, 25 July 2022, https://www.datacenterdynamics.com/en/news/global-shortage-of-fiber-optic-cables-leads-to-delays-price-increases/ See also note 47 above.

[54]Communication with industry experts, November 2022. See also note 47 above.

[55]ICPC (2022), "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables", https://www.iscpc.org/documents/?id=3733; Andy Palmer-Felgate et al. (2013), "Marine Maintenance in the Zones—A Global Comparison of Repair Commencement Times', https://minz.org.nz/i/2018-challenges/Marine-maintenance-in-the-zones.pdf.

Until recently, the most common form of intentional damage to cables was associated with theft of the actual cable materials, copper in particular.[56] Arguably terrestrial networks face somewhat similar challenges, as lengths of cables are often stolen under the misguided belief that they contain copper, although the comparison stops there since repairing subsea cable damage is much more costly and time-consuming. There have also been concerns that terrorist groups could disrupt critical infrastructure, including critical communications infrastructure such as submarine cables. These concerns even made it into a Security Council resolution, but no such event has ever transpired, at least to public knowledge.[57]

More visible recently, however, are the existing and potential threats posed by States to undersea communications cables. Such threats have a long history. For instance, prior to the negotiation of the 1884 Convention for the Protection of Submarine Telegraph Cables, State intervention in cable projects increased significantly in tandem with the territorial expansionism of the time. Competition for access to the resources critical to the functioning of cables intensified. Cable tapping and sabotage became a feature of conflict—first in the context of civil unrest, and then in international conflicts, with the major powers gradually integrating cable tapping and sabotage into war planning.[58] The effects when major war broke out were significant, even then, when the world was not as reliant on information technologies. Today, while a risk-management approach guides most cable projects and high redundancies are built in to ensure their availability or relatively speedy recovery in the event of failure, the situation is not so straightforward. The speed of recovery diminishes for countries that are more remote and have single points of failure. Recovery would likely also diminish in the event of an effort to disrupt critical choke points, block access to repair ships and spare part depots, or disrupt supply chains.

Many of the State behaviours noted above are visible today, reflecting the strong and worrying geopolitical currents of our time. On land they include reports of cyber operations targeting cable land facilities, and Internet exchange points;[59] of competition for control of or destruction

---

[56]See, for instance, Robert Martinage (2015), "Under the Sea: The Vulnerability of the Commons", Foreign Policy 94:1 Mick P. Green and Douglas R. Burnett, "Security of International Submarine Cable Infrastructure: Time to Rethink?", International Cable Protection Committee, p. 5, https://www.iscpc.org/documents/?id=2974.

[57]Security Council, UN document S/RES/2341 (2017); see also the United Nations Secretary-General's 2017 message for the Security Council open debate on "protection of critical infrastructure against terrorist attacks", https://www.un.org/sg/en/content/sg/statement/2017-02-13/secretary-generals-message-security-council-open-debate-protection.

[58]Camino Kavanagh (forthcoming), "The ties that bind… And the geopolitics that can unwind", SubOptic Telecoms Conference, March 2023.

[59]See, for instance, CyberScoop (2022), "DHS Investigators Say They Foiled Cyberattack on Undersea Internet Cable in Hawaii", https://www.cyberscoop.com/undersea-cable-operator-hacked-hawaii/; Colin Wall and Pierre Morcos (2021), 'Invisible and Vital: Undersea Cables and Transatlantic Security', CSIS, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security; Devirupa Mitra (2022), "Snooping Storm Brews in Mauritius Over Indian Team Accessing Internet Landing Station", The Wire, https://thewire.in/diplomacy/mauritius-snooping-storm-india-internet; Reuters (2021), "U.S. Spied on Merkel and Other Europeans through Danish Cables—broadcaster DR", https://www.euronews.com/2021/05/30/us-denmark-defence; Olga Khazan (2013), "The Creepy, Long-Standing Practice of Undersea Cable Tapping", The Atlantic, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/; and Yuval Shavitt and Chris C. Demchak (2022), "Unlearned Lessons from the First Cybered Conflict Decade—BGP Hijacks Continue", Cyber Defense Review 7:1,

of a cable systems' land facilities in live conflicts;[60] and of companies and individuals providing material support and intelligence to espionage agencies.[61] At sea, they include reported incidences of suspicious activity in the territorial waters or exclusive economic zone of several States.[62]

They also include reports of intentional State-backed cable sabotage (examples of which still fortunately remain few) as well as concerns about the potential effects of such activity on military operations.[63] It is broadly assumed that the further out to sea, the greater the chance that a major power is involved, since significant technological and maritime capabilities and resources are required to reach and access the cables. This would be the case with cable tapping on the high seas, although developments in optical sensing techniques and data encryption are, reportedly making it more difficult to detect and prevent such activity.[64]

These physical and cyber threats—happening against a background of increasing technological competition among States—are in turn increasingly referenced or inferred in national and regional policies and strategies,[65] and in bilateral cooperative agreements between States.[66] They are increasing research and development expenditures in naval capabilities and strategic technologies to enable, monitor and deter activity that could affect subsea cable systems, or confer an advantage over other States in this area.[67] The threats are prompting legislative

---

[60]See Celine Alkhaldi and Mostafa Salem (2022), "Airstrikes Kill 70 People and Knock out Internet in Yemen", CNN, https://edition.cnn.com/2022/01/21/middleeast/yemen-detention-strike-internet-outage-intl/index.html; Recorded Future (2018), "Underlying Dimensions of Yemen's Civil War: Control of the Internet", https://go.recordedfuture.com/hubfs/reports/cta-2018-1128.pdf.

[61]In 2018 the US Treasury Department sanctioned five Russian firms and three Russian nationals alleged to have provided support to the Russian Federal Security Service in tracking underwater fibre-optic cables; Morgan Chalfant and Olivia Beavers (2018), "Spotlight Falls on Russian Threat to Undersea Cables", The Hill, https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables/.

[62]CSIS (2022), 'What Lies Beneath: Chinese Surveys in the Maritime Sea', https://amti.csis.org/what-lies-beneath-chinese-surveys-in-the-south-china-sea/; Huong Le Thu and Bart Hogeveen (2022), "UK, Australia and ASEAN Cooperation for Safer Seas", ASPI, https://www.aspi.org.au/report/uk-australia-and-asean-cooperation-safer-seas; Naomi O'Leary (2022), "Ireland's Crucial Submarine Cables are Vulnerable to Attack", The Irish Times, https://www.irishtimes.com/world/europe/2022/09/28/irelands-submarine-cables-are-vulnerable-to-attack/; Office of the Director of National Intelligence (2022), 'Annual Threat Assessment of the US Intelligence Community', https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

[63]Atle Staalesen (2022), "'Human Activity' behind Svalbard Cable Disruption", The Barents Observer, https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption; Rishi Sunak (2017), "Undersea Cables: Indispensable, Insecure", Policy Exchange, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf; Regarding military operations abroad, see Michael Sechrist (2010), "Cyberspace in Deep Water: Protecting Undersea Communications Cables by Creating an International Public–Private Partnership", Harvard Kennedy School. Sechrist discusses how in late 2008, three cables between Italy and Egypt were severed reportedly resulting in a significant reduction in US UAV operations in Iraq.

[64]Cable tapping was a practice of all major naval powers in the pre-fibre optic era. In comparison to the copper and coaxial cables of yore, it is more difficult to physically tap today's fibre optic cables and the repeaters. Special equipment reportedly only available to a handful of States would be required. This includes specially equipped submarines, or submersibles operating from ships, and a capacity to stealthily exfiltrate and decrypt the data in the cables. Conversely, a cable system's land infrastructure and network management systems are much more vulnerable to espionage activity. While important efforts are underway to harden the physical and cybersecurity of these, full protection including from insider threats and domestic political decisions, will always be challenging.

[65]See, for example, U.S. Executive Order 13873 (2019) on Securing the Information and Communications Technology and Services Supply Chain; France Ministère des Armées (2022), Ministerial Strategy for Seabed Warfare, https://archives.defense.gouv.fr/content/download/636000/10511901/file/20220214_FRENCH%20SEABDED%20STRATEGY_key%20points.pdf; Directive (EU) 2022/2555 of 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555; NATO (2023), "NATO Stands up Undersea Infrastructure Coordination Cell", https://www.nato.int/cps/en/natohq/news_211919.htm. This follows the earlier announcement of a joint EU–NATO taskforce: NATO (2023), "NATO and the EU Set up Taskforce on Resilience and Critical Infrastructure", https://www.nato.int/cps/en/natohq/news_210611.htm.

decisions to increase investments in cable repair capabilities[68] and research and development for trusted cable technology and networks for military/defence communications. They are also the reason why new taskforces and coordination structures are being stood up in certain regions.[69] In addition, many States are more actively intervening in cable projects to influence choices on cable routing, technologies and financing on the grounds of national security,[70] resulting in lengthier licensing and permitting processes. In some cases, States block specific projects if certain companies are involved, or if the cables land in or connect to certain jurisdictions (see Box 1 below).

Such decisions blend with similar national or regional security-guided decisions to include subsea communications cable-related technologies in critical and emerging technologies lists and export controls lists,[71] or to invest in subsea cable and other digital infrastructure projects in strategically important maritime regions such as the Atlantic Ocean, the Baltic Sea, the Mediterranean, the Indo-Pacific, the Northwest Passage, the South China Sea, or commercially important data-rich regions such as Africa and South-East Asia.[72]

In short, subsea communications cables are becoming an important feature of geopolitical contestation, with considerable implications for the security and resilience of cables and the broader ICT ecosystem upon which the functioning and well-being of our societies increasingly relies. Which begs the question: is the current subsea cable regime fit for purpose?

---

[66]See, for instance, the 2020 Australia–Singapore Digital Economy Agreement, para. 22, https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf; and the 2022 UK–Singapore Digital Economy Agreement, § 7, Additional Provisions, "Submarine Cable Landing Systems", https://www.gov.uk/government/publications/uk-singapore-digital-economy-agreement-explainer/uk-singapore-digital-economy-agreement-final-agreement-explainer. The U.S.–EU Trade and Technology Council also intends to discuss subsea communications cables under the framework of its Working Group on ICT security and competitiveness. Issues that will be discussed include transatlantic subsea cables' connectivity and security, including alternative routes, such as the transatlantic route to connect Europe, North America and Asia; supplier diversification efforts in ICT supply chains; and market trends towards open, interoperable approaches, alongside trusted, established architectures; see the 2022 US–EU Joint Statement of the Trade and Technology Council, heading "Future Secure Connectivity Projects", https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/.

[67]Charlotte le Breton and Hugo Decis (2022), "France's Deep Dive into Seabed Warfare", IISS Military Balance Blog, https://www.iiss.org/blogs/military-balance/2022/02/frances-deep-dive-into-seabed-warfare; Martina Bet (2022), "Ben Wallace: Specialist Ships Will Protect Underwater Cables from Russia", Evening Standard, https://www.standard.co.uk/news/politics/ben-wallace-moscow-russia-keir-starmer-government-b1029675.html; Jonathan Beale (2021), "New Royal Navy Ship to Protect 'Critical' Undersea Cables", BBC News, https://www.bbc.com/news/uk-56472655; Alexandra Brzozowski (2020), "NATO Seeks Ways of Protecting Undersea Cables from Russian Attacks", Euractiv, https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/; and Dimitrios Eleftherakis and Raul Vicen-Bueno (2020), "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors", Sensors 20:3, https://www.mdpi.com/1424-8220/20/3/737.

[68]In 2019, the US National Defense Authorization Act for Fiscal Year 2020 provided for the establishment of a 'Cable Security Fleet'; for a discussion on challenges relevant to operationalizing the fleet, see Douglass R. Burnett (2022), "Repairing Submarine Cables Is a Wartime Necessity", Proceedings 148:10, https://www.usni.org/magazines/proceedings/2022/october/repairing-submarine-cables-wartime-necessity.

[69]See footnote 67.

[70]Hilary McGeachy (2022), "The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns", Australian Journal of International Affairs 76:2.

[71]See, for example, US National Science and Technology Council (2022), "Critical and Emerging Technologies List Update", p. 4, https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

[72]For a broader insights int subsea cable infrastructure investments, see footnotes 68, 72 and 138.

Box 1: A decade of reactive routing decisions

- Efforts by BRICS States to build a submarine cable connecting each other so as to avoid the heavy costs of routing through Europe and the United States, and potential interception of critical financial and security information by non-BRICS entities. Despite positive market, traffic and feasibility studies, the cable project did not go ahead. https://www.offshore-energy.biz/brics-unveils-new-submarine-cable-system/

- Brazil's efforts to seek alternative routes, including with the European Union, as to avoid routing traffic through the United States (2014).
https://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224

- Australia's decision to pay for a 4,000 km subsea cable connecting Australia, Solomon Islands and Papua New Guinea (2018).
https://www.bbc.co.uk/news/world-australia-44463553

- The decision of Chile to route a cable to Australia, rather than Asia (2020). https://www.datacenterdynamics.com/en/news/chiles-transoceanic-cable-connect-new-zealand-and-australia/

- The [US Team Telecom] recommendation to the US Federal Communications Commission that it deny the Pacific Light Cable Network's Hong Kong undersea cable connection to the United States (2020).
https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea

- The decision by companies to refile or withdraw landing licensing applications for trans-Pacific cable projects landing in Hong Kong (2020–2021).
https://blog.telegeography.com/trans-pacific-cables-asian-hubs-plcn-status

- The decision by the Russian Federation on the Polar Express cable project, intended to connect the Arctic communities along the Northwest coast (2021).
https://www.capacitymedia.com/article/29otdhk3j2ycxulos7b40/news/russia-begins-889m-polar-express-arctic-cable

- The decision to develop the Far North Fibre Express Route—a multicontinent cable project through the Northwest Passage rather than the previously projected Arctic Connect project that would have run through the Northeast Passage (2022).
https://www.thearcticinstitute.org/geopolitics-subsea-cables-arctic/

- The [US Team Telecom] recommendation to the US Federal Communications Commission, regarding a proposed modification to the ARCOS-1 cable system to include an authorized landing point in Cuba, recommending that the connection be denied (2022).
https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through

- The announcement by Cuban State-run telecommunications operator ETESCA that it had begun work with French telecoms operator Orange, to provide the country with an additional link, via French overseas territory Martinique (2022).
https://www.reuters.com/business/media-telecom/cuba-french-telecoms-operator-orange-begin-work-subsea-cable-martinique-2022-12-08/

- The decision by Chinese telecommunications companies – China Telecom and China Mobile - to withdraw their investment in the Sea-Me-We 6 cable project after the decision to award the build to a U.S. company in lieu of a Chinese one (2022) https://www.ft.com/content/8f35bf1e-fe32-4998-9e13-a13bac23506d

The Regime Governing Subsea Communications Cables

The extant cable governance regime is made up of a patchwork of international treaties, regulatory frameworks, international and regional organizations, industry associations, protocols, standards and best practices.[73] One of the main subsea cable bodies, the International Cable Protection Committee (ICPC), is a forum where owners, operators and suppliers of subsea telecommunications or power cables and government representatives share technical, legal and environmental information. The organization has more than 190 members from more than 69 countries and represents more than 98 per cent of the world's subsea telecommunications cables. It promotes awareness of submarine cables as critical infrastructure, issuing best practices for cable protection and resilience, provides guidance on technical and regulatory issues and recommendations for cable installation, protection and maintenance.[74] Government participation in ICPC is welcomed and has grown in past years, yet it remains minimal. Smaller associations exist at the regional level including, for example, the European Submarine Cables Association (ESCA), the North American Cable Association (NASCA) and the Oceania Submarine Cable Association (OSCA).[75]

From a government policy perspective, subsea cable protection straddles a range of areas including maritime security, internal affairs or homeland security, defence, cybersecurity, digital, communications, trade, investment and industrial policy. There is no international arrangement for subsea cable governance yet, as noted, some regional organizations such as the Association of Southeast Asian Nations and the European Union cover various governance aspects.[76]

The anchor for government involvement (and responsibilities) in the protection of subsea cables can be found in existing international law. Indeed, subsea cables have been addressed in several conventions, the first of which dates back to the late nineteenth century. These include:

- The 1884 Convention for the Protection of Submarine Telegraph Cables.[77]
- The 1907 Convention Respecting the Laws and Customs of War on Land and its annex:

---

[73]Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", Contemporary Security Policy 42:3.

[74]See https://www.iscpc.org .

[75]For details on their respective mandates and membership, see ESCA, https://escaeu.org; NASCA, https://www.n-a-s-c-a.org; and OSCA, http://www.oscagroup.com. Another such committee is the Danish Cable Protection Committee, which brings together subsea industry actors, including telecommunications, working in Danish maritime waters.

[76]See footnotes 8 and 42.

[77]For the full text, see https://www.iscpc.org/documents/?id=13.

[78]Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land (1907), regulations: art. 54, https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907.

Regulations concerning the Laws and Customs of War on Land.[78]

- The 1958 Convention on the High Seas[79] and the 1958 Convention on the Continental Shelf.[80]
- The 1982 United Nations Convention on the Law of the Sea (UNCLOS),[81] which supersedes the latter two and establishes three areas of maritime jurisdiction where cables are concerned: territorial seas, the exclusive economic zone and the high seas.[82]

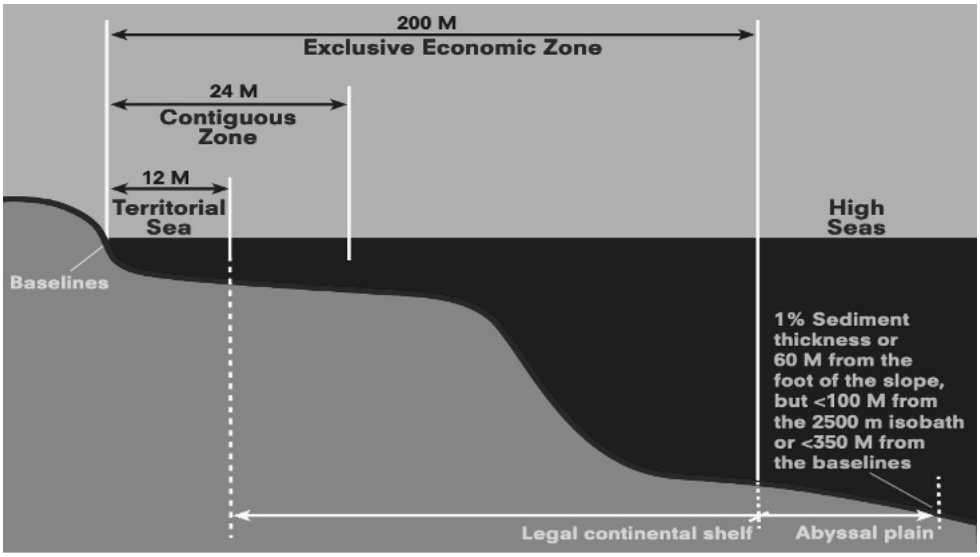


Figure 4. UNCLOS Maritime Zones[83]

Today UNCLOS remains the main point of reference on subsea cables (see Annex 1 for relevant provisions). UNCLOS permits States to lay cables in the high seas, in the exclusive economic zone, and on the continental shelf, and to repair cables (art. 79). It includes provisions on breaking and injury of subsea cables (arts. 113, 114) and on indemnity for loss (art. 115). As with the Convention on the High Seas, art. 113 calls on States parties to adopt domestic legislation penalizing damage to cables beneath the high seas by ships flying its flag or persons under their jurisdiction. It also expands the scope of a punishable offence to include "conduct calculated or likely to result in … breaking or injury [of a subsea cable]", a provision that has been interpreted as allowing States "to act to prevent cable breaks from occurring".[84]

Challenges abound, though, where legal cover and adherence are concerned. To start, not all States are party to UNCLOS. Also, the Convention does not give adequate jurisdiction over offenders or the ability to board suspect vessels, as civil and criminal jurisdiction in the event of damage to a cable is limited to the home State of the responsible individual or to the flag State

[79]Articles 1, 26–30; for the full text, see https://www.iscpc.org/documents/?id=14.
[80]Article 4; for the full text, see https://www.iscpc.org/documents/?id=16.
[81]Articles 3, 21, 33, 57–58, 79, 86–87, 112-115, 297; for the full text, see https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm.
[82]Lane Burdette (2021), "Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy", Journal of Public and International Affairs, https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy.
[83]United Nations (2013), "UNCLOS at 30", p. 4, https://www.un.org/depts/los/convention_agreements/pamphlet_unclos_at_30.pdf.
[84]Eric Wagner (1995), "Submarine Cables and Protections Provided by the Law of the Sea", Marine Policy 19:2, p. 136.

of the responsible vessel.[85] The 1884 Convention for the Protection of Submarine Telegraph Cables included a provision entitling any warship suspecting a foreign vessel of damaging a cable to "demand from the captain or master the production of the official documents proving the nationality of the said vessel".[86] Yet, a rule to that same effect was not included in either the 1958 Conventions or in UNCLOS.[87] Furthermore, while under UNCLOS all States are required to adopt laws that make the willful or culpably negligent infliction of damage to a subsea cable a punishable offence, few States have yet to do so in any meaningful way.[88] Where they have, such efforts have been described as "woefully inadequate and not commensurate with the damage resulting from intentional interference".[89] And, importantly, many States do not adhere to the UNCLOS provision regarding maintenance and repair, imposing lengthy repair-permitting processes the effects of which some have described as being comparable to sabotage.[90]

Other gaps exist, particularly in regard to cable protection during conflict. A specific provision on belligerent activity was included in the 1884 Convention, yet this permits rather than restricts the freedom of action of belligerents.[91] UNCLOS did not take up this matter. The only other instrument that deals with submarine cables during conflict is the 1907 Convention.[92] Its article 54 provides special protections for submarine cables (including land components) connecting occupied with neutral territory, noting that they may not be seized or destroyed except in the case of absolute necessity and that compensation must immediately be paid. [93] The San Remo Manual on International Law Applicable to Armed Conflicts at Sea echoed this sentiment, stating that "belligerents shall take care to avoid damage to cables and pipelines laid on the sea-bed which do not exclusively serve the belligerents".[94] However, subsea cables today transmit data of value to all States, even when cables do not directly land on their territory, raising questions about the continued relevance of the provision to undersea

---

[85] See relevant commentary in Yoram Dinstein and Arne Willy Dahl (eds) (2020), Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary, rule 67, pp. 61ff; see also Rishi Sunak (2017), "Undersea Cables: Indispensable, Insecure", Policy Exchange, p. 6, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf.

[86] Article X, 1884 Convention for the Protection of Submarine Telegraph Cables.

[87] Communication with Prof. Dr. Wolff Heintschel von Heinegg, Chair of Public Law, in particular Public International Law, European Law and Foreign Constitutional Law, Europa-Universität Viadrina, 19 January 2023.

[88] Michael N. Schmitt (ed.) (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, rule 54, para. 19, p. 258.

[89] Tara Davenport (2015), "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis", Catholic University Journal of Law and Technology 24(1).

[90] Lane Burdette (2021), "Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy", Journal of Public and International Affairs, p. 4, https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy; Hai Dang Vu (2020), "ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables", The International Journal of Marine and Coastal Law 36:1.

[91] "It is understood that the stipulations of the present Convention do not in any way restrict the freedom of action of belligerents", art. XV, 1884 Convention for the Protection of Submarine Telegraph Cables.

[92] Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land (1907), https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907.

[93] Ibid., regulations: art. 54.

[94] San Remo Manual on International Law Applicable to Armed Conflicts at Sea (1994), para. 37. Note that the San Remo Manual is a "contemporary restatement of international law applicable to armed conflicts at sea" developed by a group of legal and naval experts in their personal capacity between 1988 and 1994; see https://ihl-databases.icrc.org/en/ihl-treaties/san-remo-manual-1994.

communications cables.[95] Experts also question whether an attack on a subsea cable beyond a State's jurisdiction would qualify as an armed attack for the purposes of article 51 of the Charter of the United Nations, which would permit the use of force by a State in self-defence.

A number of initiatives have addressed these gaps, and also considered new developments such as cyber operations affecting subsea cables. Some of this work has informed publications such as the Tallinn Manual on the International Law Applicable to Cyber Operations and the Oslo Manual on Select Topics of the Law of Armed Conflict. For instance, the Tallinn Manual 2.0 notes that UNCLOS is applicable to cyber operations conducted from or through cyber infrastructure located in the seas, determining that "cyber operations may be deployed from ships and vessels at sea, aircraft above the seas, offshore installations, or through submarine communications cables, both in peacetime and in conflict".[96] It concludes that "existing international law applying to submarine cables, including submarine communications cables, and the operation thereof, generally reflects customary international law",[97] viewing submarine communications cables as any "cable owned, operated or laid by a State, as well as privately owned cables, authorized by that State for telecommunications and data traffic".[98] Regarding UNCLOS article 113, the Oslo Manual concludes, that "States having laid submarine cables …, or whose nationals have laid and operate such cables … are entitled to take protective measures with a view of preventing or terminating any harmful interference".[99] And the Tallinn Manual 2.0 concludes that a cyber operation damaging a subsea cable is prohibited under customary international law, although it implies that the subsea cables may be targeted in the context of an armed conflict, subject to the principles of distinction and proportionality.[100] It also suggests that a cyber attack conducted via a subsea communications cable in the context of an armed conflict would render the cable a lawful target. Both manuals determine that modern communications cables raise questions about article 54 of the 1907 Convention, with the Oslo Manual specifically noting that, "it will only in rare circumstances be possible to determine that they are exclusively serving one or more belligerents", hence the importance of "distinguishing between submarine communications cables and other submarine cables".[101]

Several scholars have advocated for additional international legal cover for activity affecting

[95]The Tallinn Manual 2.0 pays specific attention to this provision, noting that "since submarine cables facilitate cyber communications, the point has particular relevance to the cyber context"; Michael N. Schmitt (ed.) (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, rule 150, para. 10, p. 549. See also Lane Burdette (2021), "Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy", Journal of Public and International Affairs, p. 3, https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy, who highlights "the U.S. precedent, later upheld in a 1923 U.S.–U.K. arbitration tribunal, permits offensively cutting cables between target and neutral States within a target EEZ", which is not reflected in the assessment of the Tallinn Manual experts.

[96]Michael N. Schmitt (ed.) (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, rule 54, para. 1, pp. 252–253.

[97]Ibid., pp. 252–258.

[98]Ibid.

[99]Yoram Dinstein and Arne Willy Dahl (eds) (2020), Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary, rule 67, p. 61.

[100]Michael N. Schmitt (ed.) (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, rule 54, para. 15, p. 256.

[101]Yoram Dinstein and Arne Willy Dahl (eds) (2020), Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary, rule 69, p. 63.

subsea cables, including the negotiation of a new instrument.[102] To this end, some have suggested "using the structure of the [United Nations] counter-terrorism conventions" as a guide.[103] Others have taken a more limited approach, suggesting new UNCLOS provisions that would clarify responsibilities, obligations and compliance measures, and strengthen mutual cooperation on enforcement against criminal activity.[104] Other more limited approaches have proposed establishing cable protection zones in coastal areas with high-value communications corridors, although this might make the cables more vulnerable than they already are.[105]

Some scholars have also suggested establishing an international agency under the umbrella of the United Nations system with legal and policy responsibility for subsea cables.[106] Others have proposed using the binding dispute resolution system of the International Tribunal for the Law of the Sea "to create an international regime to protect against submarine cable damage" and "against violations of the right to privacy".[107] Meanwhile, academic proposals more focused on the international law applicable to subsea cables during armed conflict include suggestions to amend the 1884 Convention provision on belligerent activity to prohibit intentional damage by physical or cyber means. Another proposes yet another convention, placing subsea communications cables under special protection during conflict, similar to the protections for cultural property during armed conflict.[108] Others have suggested modifying the application of the ordinary rule of proportionality in targeting.[109]

---

[102]Robert Beckman, "Protecting Submarine Cables from Intentional Damage: the Security Gap", in Douglas R. Burnett, et al. (eds) (2013), Submarine Cables: The Handbook of Law and Policy, BRILL; Tara Davenport (2015), "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis", Catholic University Journal of Law and Technology 24(1); Zoe Scanlon (2017), "Addressing the Pitfalls of Exclusive Flag State Jurisdiction: Improving the Legal Regime for the Protection of Submarine Cables", Journal of Maritime Law and Commerce 48:3; Rishi Sunak (2017), "Undersea Cables: Indispensable, Insecure", Policy Exchange, pp. 35–36, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

[103] Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", Contemporary Security Policy 42:3, p. 398.

[104]Tara Davenport (2015), "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis", Catholic University Journal of Law and Technology 24(1).

[105]Rishi Sunak (2017), "Undersea Cables: Indispensable, Insecure", Policy Exchange, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf. In its Best Practices for Government, the ICPC has recommended against establishing cable protection zones and corridors within fixed geographic areas, or at minimum suggests engaging in consultations with cable operators when taking such an approach. The latter tend to be against such protection zones and corridors as they "(1) provide insufficient spatial separation from other submarine cables for installation and maintenance and (2) encourage geographic clustering of submarine cable routes and landings, which magnifies the risk that a single natural or man-made event could damage multiple cables"; ICPC (2022), "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables", p. 3, https://www.iscpc.org/documents/?id=3733.

[106]Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", Contemporary Security Policy 42:3, p. 399.

[107]Jason Petty (2021), "How Hackers of Submarine Cables May Be Held Liable Under the Law of the Sea", Chicago Journal of International Law 22:1.

[108]For example, the 1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict (itself guided by the principles concerning the protection of cultural property during armed conflict, the Hague Conventions of 1899 and 1907; and the Washington Pact of 1935); see Dennis E. Harbin III (2021), "Targeting Submarine Cables: New Approaches to the Law of Armed Conflict in Modern Warfare", Military Law Review 229, https://tjaglcs.army.mil/documents/35956/304883/3+Harbin+Final.pdf.

[109]See Rob McLaughlin, Tamsin Phillipa Paige and Douglas Guilfoyle (2022), "Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization", Journal of Conflict and Security Law 27:3.

Whither Subsea Cable Governance?

There is a strong basis for arguing that the extant subsea cable governance regime is insufficient to meet the challenges of this century. There is an equally strong basis for arguing that a new global instrument is necessary, particularly given our dependency on subsea cables for connectivity and the reality that existing instruments do not reflect the nature of current technologies. Yet, many experts would insist that existing international law is sufficient, and that States need to adhere to existing obligations and commitments before even considering a new instrument. And even if States were to agree on the need for a new treaty specifically focused on protecting subsea cables, it would likely take decades to negotiate because it would be difficult to agree on its scope given that subsea cable systems are just one, albeit critical, element of the broader ICT ecosystem. As noted, more limited approaches focused on strengthening existing instruments have been suggested. These each have their value and should be studied further.

There are other, complementary ways to strengthen the governance regime and the resilience of subsea cable systems. For instance, there is the option of increased involvement of the military in cable protection and security, including through dedicated coordination structures; underwater sensing and surveillance and maritime surface patrols in, as well as satellite surveillance of, strategically relevant waters.[110] And there is the option of stronger regulation, particularly with regard to ensuring the use of trusted technologies, to ensuring sovereign capabilities for maintenance and repair,[111] and to increasing information-exchange with cable owners and operators.[112] Important as they are, these different approaches respond to the resilience and security concerns of certain countries or regions. They need to be accompanied by efforts to strengthen resilience of subsea communications cables at the global level.

Perhaps a starting point for such a global conversation would be to recognize the systemic nature of the challenges at hand and deepen understanding of the risk mitigation efforts that industry and technical communities are already taking (e.g., greater diversification of cable routes and capacity; uptake of zero-trust principles and technologies, hardening the security of land infrastructure and components, advancing optical sensing techniques for system monitoring). States can complement these efforts by advancing implementation of and

---

[110]For example, the new NATO coordination cell announced on 15 February 2022; see also Rishi Sunak (2017), "Undersea Cables: Indispensable, Insecure", Policy Exchange, pp. 35–36, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf, pp. 35-36; Andreas Rinke and Matthias Williams (2022), 'Germany and Norway Want NATO to Protect Subsea Infrastructure after Nord Stream Attacks", Reuters, https://www.reuters.com/business/energy/germany-norway-ask-nato-protect-subsea-infrastructure-after-nord-stream-attacks-2022-11-30/.

[111]Ian Douglas (2021), "Future Proofing the UK's Critical Subsea Cable Infrastructure', Global Marine Group, https://nationalpreparednesscommission.uk/2021/09/future-proofing-the-uks-critical-subsea-cable-infrastructure/.

[112]See, for instance, Directive (EU) 2022/2555 of 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555.

adherence to existing recommendations and emerging requirements relevant to critical ICT infrastructure. These include:

- the ICPC best practices for protecting and promoting resilience of submarine telecommunications cables, the essence of which derive from UNCLOS, and its upcoming recommendation on the security of beach manholes, front haul, and cable landing stations;
- relevant elements of the framework for responsible State behaviour negotiated at the United Nations with regard to ICTs and international security;[113] and
- new requirements emerging at national and regional levels, including under the European Union's Network and Information Systems Directive.[114]

Such a focus will not resolve some of the thornier geopolitical issues discussed herein such as the signalling by some States that they can put critical infrastructure such as subsea cables systems at risk for their own gain. It can nonetheless advance efforts to protect and secure the systems, and the terrestrial and satellite networks they connect to, thus enhancing their resilience and their capacity to deliver on much-needed economic and social dividends.

[113]See, for example, https://www.un.org/disarmament/ict-security/.
[114]For example, Directive (EU) 2022/2555 of 14 December 2022, https://eur-lex.europa.eu/eli/dir/2022/2555.

Analysis of Selected Efforts

The ICPC Government Best Practices are recommendations developed on the basis of existing international law and policy, industry protocols and standards, State practice, and basic common sense.[115] They cover a range of issues. For instance, the general principles (§ 1) suggest that in their national resilience plans, States should focus on:

- statistically significant risks where government action could have the greatest impact on risk reduction;
- diversification of subsea cable landings within the State's jurisdiction;
- observation and implementation of existing obligations and customary international law defining State jurisdiction over, and protection of, submarine cables;
- promotion of transparent regulatory regimes that expedite cable deployment and repair according to well-established timeframes;
- close consultations with industry to understand industry technology and operating parameters and to share data regarding risks;
- complementing existing industry best practices;
- recognizing that laws and government policies themselves can sometimes exacerbate risks of damage and reduce resilience; and
- engaging with other States on a global and regional basis, as other States' actions can greatly affect an individual State's own connectivity.

The ICPC best practices provide more detailed guidance across various subject areas, all of which are relevant to strengthening resilience. For instance, the recommendations that States designate subsea cables as critical infrastructure,[116] gather and assess data regarding vulnerabilities and threats and develop and implement policies to reduce these, would likely resonate with all States. It would also help to prioritize attention and resources and help to differentiate between unintentional risks and those implicating national and international

[115] ICPC (2022), "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables", https://www.iscpc.org/documents/?id=3733.

[116] Ibid, § 4, p. 5, notes that International Hydrographic Organization resolution 4/1967 requires national and regional charting authorities to include a text box in all nautical charts setting minimal distances for operating near cables and "recognizing submarine cables as critical infrastructure", damage to which "can constitute a national disaster" [emphasis added]; see also the discussion of spatial separation in ibid., § 3, which also addresses implementation of the resolution.

security. Establishing a single point of contact to better coordinate government action across the lifecycle of a cable, basic parameters for installation and repair permitting, and mechanisms for exchanging incident data and threat information between cable operators and government would also be significant steps forward.

Results could also be achieved by implementing the recommendation on domestic cable protection laws in a manner consistent with UNCLOS. This would help to ensure meaningful penalties for damage. Coast guards and other relevant law enforcement authorities would become "sufficiently familiar with cable protection laws to enforce them, and … cooperate with and assist cable operators in investigating cable damage claims".[117] Similarly, deepening government understanding of spatial separation, routing and landing issues can help to protect against bad policy decisions, and accelerate the adoption of much-needed regulatory frameworks and resource allocations in this area.[118] Moreover, greater clarity on how States are implementing these recommended practices, as well as challenges encountered, would be an important contribution to the current discussion. So too would learning from the United Nations Office on Drugs and Crime's efforts and those of other organizations to support Member States implementing these best practices.[119]

ICPC Government Best Practices for Cable Protection and Resilience	1. General principles
	2. Fishing and anchoring risks (70% of faults)
	3. Spatial separation
	4. Charting
	5. Domestic cable protection laws; penalities for damage
	6. Marine spatial planning and inter-industry coordination
	7. Single point of contact
	8. Route and landing optimization; geographic diversity
	9. Permitting for installation and repair
	10. Cabotage and crewing restrictions
	11. Port entry requirements
	12. Customs duties, taxes, and fees
	13. Maritime boundary claims and disputes
	14. Critical infrastructure designation
	15. Sharing of risk and incident data
	16. Impact of other high-seas regulatory activities.

Table 1. ICPC Best Practices for Governments

Beyond these best practices, ICPC's Cable Security Working Group is also working to develop a recommendation for protection of unique elements of subsea cable infrastructure, for example, beach manholes, fronthaul, and cable landing stations. The recommendation does not cover cyber or information security-related issues, recognizing that "security of

[117]Ibid, § 5.

[118]Ibid., e.g., §§ 3, 6 and 8.

[119]See, for example, Kaithlin Meredith (2021), "Protecting Submarine Cables in the Indian Ocean", UNODC, https://www.unodc.org/easternafrica/en/Stories/protection-of-submarine-cables-in-indian-ocean.html.

communications themselves is not a unique issue for subsea cables and is otherwise addressed in cybersecurity for electronic communications networks, such as ISO 27001 and national level standard-setting cybersecurity frameworks".[120] Promoting this recommendation once released, as well as relevant exchanges on implementation progress, will also be an important contribution.

Where cybersecurity is concerned, a number of international developments are also worth considering. For instance, the General Assembly First Committee negotiations on ICTs and international security have resulted in an emerging framework for responsible State behaviour, elements of which refer concretely to critical infrastructure protection.[121] Indeed, the first of three critical infrastructure-related norms recommended by the GGE in 2015 relates to the responsibility of States "to not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public".[122] In its explanation of the types of critical infrastructure that may be inferred under this norm, two later reports clarified that it may refer to those infrastructures that provide services across several States, such as "the technical infrastructure essential to the general availability and integrity of the internet", which, by a broader ICT ecosystem logic, would include subsea communications cables.[123]

Equally applicable are the other two critical infrastructure-related norms recommended in the same report, notably that "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199";[124] and that "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical

[120]Communication with ICPC representative, 17 January 2022.

[121]For the relevant reports, see General Assembly, UN document A/70/174 (2015), https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf; General Assembly, UN document A/76/135 (2021), https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf; and General Assembly, UN document A/AC.290/2021/CRP.2 (2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[122]General Assembly, UN document A/76/135 (2021), norm 13(f), paras. 42–46, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

[123]Ibid. This language on the "technical infrastructure essential to the general availability or integrity of the Internet" stems from proposals by the Netherlands relevant to the public core of the Internet, which in turns draws from the work of Dutch scholar Dennis Broeders on the topic, later taken up by the Global Commission on the Stability of Cyberspace in its proposal for a norm to protect the public core of the Internet. For the relevant United Nations reports, see footnote 122 above. For the Broeders publication, see Dennis Broeders (2016), The Public Core of the Internet: An International Agenda for Internet Governance, Netherlands Scientific Council for Government Policy, https://library.oapen.org/bitstream/handle/20.500.12657/32439/610631.pdf. For the report of the Global Commission on the Stability of Cyberspace and its advocacy for a norm of non-interference with the 'public core of the Internet', defined as including "such critical elements of the infrastructure of the Internet as packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media [including terrestrial and undersea cables and the landing stations, data centres, and other physical facilities which support them], software, and data centers" (pp. 30–31), see Global Commission on the Stability of Cyberspace (2019), "Advancing Cyberstability: Final Report", https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

[124]General Assembly, UN document A/76/135 (2021), norm 13(g), paras. 47–50, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

[125]Ibid., norm 13(h), paras. 51–55.

infrastructure of another State emanating from their territory, taking into account due regard for sovereignty".[125] Specific guidance on how to interpret these norms was provided in a 2021 report by another GGE, and touched upon by a broader OEWG.[126]

UN Recommended Norms on Critical Infrastructure	
	13 (f) States should not conduct or knowingly support ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
	13 (g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.
	13 (h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

Table 2. Recommended Critical Infrastructure-Related Norms, 2015 GGE

Many more recommendations and findings of the reports produced by these negotiating groups can and should be understood as applying also to subsea cables and related infrastructure. These include the assessment that existing international law, including the Charter of the United Nations, applies to the use of ICTs by States, other recommendations on norms,[127] and the recommendations on confidence-building measures relevant to critical infrastructure protection, including with regard to points of contact and exchanges between States and with the private sector on threats and vulnerabilities and on incident response.[128] Again, understanding how States are adhering to said commitments as they pertain to subsea cables and related infrastructure would be an important contribution to ongoing discussions.

At regional level, the European Union has advanced this line of thinking in its updated version of the Network and Information Systems Directive, by noting the importance of undersea communications to the "competitive digitalization of the Union and its economy".[129] Building on existing frameworks such as the European telecommunications framework, the EU Cybersecurity Act and Directive 2013/40/EU prohibiting attacks against information systems, it brings some of the information-exchange and incident-reporting recommendations

[126]See footnote 122.

[127]See, for instance, norm 13(c), the so-called 'due diligence' norm, whereby States commit to not knowingly allow their territory to be used for internationally wrongful acts using ICTs; norm 13(e), relevant to the protection of human rights; and norm 13(i) relevant to ensuring the integrity of the supply chain; General Assembly, UN document A/76/135 (2021), norm 13(g), paras. 47–50, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

[128]Ibid.

[129]Directive (EU) 2022/2555 of 14 December 2022, para. 97, https://eur-lex.europa.eu/eli/dir/2022/2555.

further, by imposing a new requirement on companies to report incidents affecting such systems and extending scope of the coverage to include telecommunications entities.[130] The Network and Information Systems Directive also calls on governments to consider cybersecurity aspects of subsea cable systems in their national cybersecurity strategies, where relevant, and to map potential cybersecurity risks and mitigation measures "to secure the highest level of their protection".[131] More specifically, it calls on member States to adopt policies "relating to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables".[132] Work is underway to deconflict these and other measures in the Directive from measures proposed in other recent instruments. Ensuring regular, two-way exchanges among relevant States and industry actors on implementing these measures will also be an important contribution to ongoing discussions.

[130]Proposal COM/2020/823 of 16 December 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0823; Directive 2002/21/EC of 7 March 2002, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021; Directive (EU) 2018/1972 of 11 December 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG; and Directive 2013/40/EU of 12 August 2013, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040.

[131]Directive (EU) 2022/2555 of 14 December 2022, para. 97, https://eur-lex.europa.eu/eli/dir/2022/2555.

[132]Ibid., art. 7, para. 2(d).

Paving the Way to Greater Resilience of Subsea Cable Systems at Global Level

What can be done to achieve greater resilience of subsea cables at global level and advance the existing framework of responsible State behaviour relevant to ICTs? Bearing the previous section in mind, a preliminary agenda could focus on the following.

Subsea Communications Cables as Critical Infrastructure

Subsea communications cables are an essential element of the ICT ecosystem. We all rely on them, whether directly or indirectly, so it is in our collective interest to ensure they are considered as such. In this regard, all relevant States, should designate subsea communications cables critical infrastructure. In addition, States can take the following steps:

- Publicly reaffirm their commitment to the three critical infrastructure-related norms and other related measures recommended at the United Nations in its work on international security and ICTs. States can publicly articulate their commitment to these measures, including as they apply to subsea cables and related infrastructure and promote adherence to them in bilateral, plurilateral or multilateral forums and agreements. In light of growing concerns regarding intentional activity involving States that intentionally damages subsea cable systems or otherwise impairs the use and operation of such infrastructure to provide services to the public, States can also advance discussion, difficult as it may be, on the consequences of such activity.

- Strengthen domestic law, regulatory frameworks and policy relevant to the protection and resilience of subsea cables and related infrastructure, in line with existing obligations and practices, and clarify the roles and responsibilities of national authorities.

- Strengthen national approaches to cable system risk management and mitigation, emergency preparedness relevant to incident response and repair, and approaches to classifying and reporting incidents affecting subsea cables and related infrastructure and components.

- Exchange experiences on implementing the ICPC recommendations and best practices for protection and resilience of subsea cables, and its forthcoming recommendation on security of land infrastructure.

- Exchange experiences of mutual cooperation in cable repair in disputed territories or during natural disasters and on facilitating cable ship repair access, with a view to determining mechanisms for crisis situations.

- Exchange experiences of coast guard and law enforcement cooperation to investigate cable disruption or other unlawful activity.

- Publish and exchange national views on how existing international law applies to the disruption or sabotage of cables in crisis and in conflict, including military operations that deliberately target subsea cable components and infrastructure, or espionage operations that cause unintentional damage, thus affecting network availability and impairing the transit of telecommunications and data traffic.

- Ensure greater sources of international support and capacity-building for vulnerable countries vis-à-vis ensuring the physical and cyber security of subsea cable infrastructure and other similar facilities and systems, and in the areas of domestic legal and regulatory development and enforcement.[133]

Strengthening Public–Private Cooperation

Private companies own and operate most subsea cable systems and have critical insights into threats and vulnerabilities affecting the systems, as well as lengthy experience managing and mitigating risk. New reporting requirements are pushing greater cooperation between public and private actors. Yet, as in other areas, these relationships come with many benefits and trade-offs. They can take time to nurture and may well start on the basis of limited trust. To ensure that new reporting requirements emerging at national and regional levels meet their resilience objective, States should engage with industry and other relevant actors to enhance mutual understanding of:

- the place of subsea cable systems in the broader ICT ecosystem;

- the incentive–accountability structures that can help to overcome current trust deficits and other barriers to data-sharing, and potential models for secure and trusted information-sharing that draw on existing best practices in other sensitive environments;

- changes in subsea communications cable system architectures and relevant dependencies;

- supply chain vulnerabilities;

- trends in faults and disruptions of subsea cable systems in order to identify potential high-risk, low-probability incidents that have a bearing on national or international security and the stability of the global financial system, and to better clarify roles and responsibilities in such cases; and

[133]Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", Contemporary Security Policy 42:3, p. 402.

- industry approaches to managing and mitigating risks to subsea cable systems and the technological and other advances that are helping to protect and build resilience of the systems.

A Comprehensive and Principles-Based Policy Agenda

There are legitimate concerns regarding the security and resilience of subsea cable systems. Over-securitizing the policy debate relevant to subsea cables can, however, be problematic. For one, the current policy trajectory risks further fracturing the global Internet and stymieing innovation and competition, the long-term consequences of which may far outweigh the benefits of a more resilient and interconnected system. Furthermore, it risks untethering the design and delivery of much-needed digital infrastructure projects in developing countries from key principles such as transparency, sustainability, and accountability. As well, it risks untethering them from core human-centric objectives such as ensuring that traditionally underserved populations can reap the social and economic dividends of greater connectivity, as per the spirit of Sustainable Development Goal 9.[134] In this regard, while maintaining a strong focus on security and resilience, States should also ensure:

- an appropriate balance in how subsea cables are addressed across policy agendas domestically, regionally and internationally;

- a more inclusive discussion on the social, economic and environmental trade-offs that may stem from national-security driven cable routing, financing and investment decisions;

- greater consultation with relevant actors in both the design and delivery of subsea cable infrastructure projects, such as those currently envisaged under different development and infrastructure initiatives;[135] and

- greater transparency on how they are applying broadly accepted principles such as sustainability and accountability in such initiatives.

---

[134]C. Kavanagh (forthcoming), "The Ties that Bind…", paper prepared for the annual SubCom conference in Bangkok.

[135]US Blue Dot Network, https://www.dfc.gov/our-work/blue-dot-network; China's Belt and RoadBelt and Road Initiative (see https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative) and related Digital Silk Road and Global Development InitiativesGlobal Development Initiatives (see https://csis-website-prod.s3.amazonaws.com/s3fs-public/event/220912_Global_Development_Initiative.pdf); EU Global Gateway Strategy, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en; G7 Partnership for Global Infrastructure Development, https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment/ ; U.S.--E.U. Joint Statement of the Trade and Technology Council', 05 December 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/.

Concluding Remarks

It is increasingly acknowledged that subsea communications cables are a critical element of the global ICT ecosystem, transmitting practically all our telecommunications and data. Their security and resilience are critical to the well-being and functioning of societies across the globe. It is also recognized that States across regions have legitimate concerns regarding the security of these cables, especially in the current environment of heightened geopolitical tensions. In consequence, the current situation calls for a more global and cooperative approach to strengthening resilience of the systems. This report highlights some of the gaps in the current cable governance regime, while shedding light on other practices and recommended measures that can contribute to their protection and resilience. Its recommendations are directed mainly at States, although it recognizes the centrality and ongoing efforts of industry and other actors to such efforts. Its recommendations suggest that all relevant States consider subsea communications cables as critical infrastructure and engage with industry actors to understand efforts already underway to enhance resilience and to determine trusted and secure means for sharing-information. They also highlight the need to ensure a more comprehensive and principles-based approach to how we consider subsea cables in policy for risk of over-securitizing the agenda. The aim is not to avoid nor critique ongoing approaches to protecting and securing subsea cable systems nationally or regionally, but rather to ensure that all States and regions contribute responsibly to ensuring a more secure and resilient ICT ecosystem.

Annex 1

UNCLOS provisions relevant to subsea cables

Article 3. **Breadth of the territorial sea.**	Every State has the right to establish the breadth for its territorial sea up to a limit not exceeding 12 nautical miles, measured from baseline determined in accordance with this Convention.
Article 21. **Laws and regulations of the coastal State relating to innocent passage.**	1. The coastal State may adopt laws and regulations, in conformity with the provisions of this Convention and other rules of international law, relating to the innocent passage through territorial sea, in respect of all or any of the following: ... (c) The protections of cables and pipelines;
Article 33. **Contiguous zone.**	1. In a zone contiguous to its territorial area, described as the contiguous zone, the coastal State may exercise the control necessary to: (a) prevent infringement of its customs, fiscal, immigration or sanitary laws and regulations within its territory or territorial sea; (b) punish infringement of the above laws and regulations committed within its territory or territorial sea. 2. The contiguous zone may note extend beyond 24 nautical miles from the baselines from which the breadth of the territorial sea is measured.
Article 57. **Breadth of the exclusive economic zone.**	The exclusive economic zone shall not extend beyond 200 nautical miles from the baselines from which the breadth of the territorial sea is measured.
Article 58. **Rights and duties of other States in the exclusive economic zone.**	1. In the exclusive economic zone, all States, whether coastal or land-locked, enjoy, subject to the relevant provisions of this Convention, the freedoms referred to in article 87 of navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and compatible with the other provisions of this Convention. 2. Articles 88 to 115 and other pertinent rules of international law apply to the exclusive economic zone in so far as they are not incompatible with this Part. 3. In exercising their rights and performing their duties under this Convention if the exclusive economic zone, States shall have due regard to the rights and duties of the coastal State and shall comply with the laws and regulations adopted by the coastal State in accordance with the provisions of this Convention and other rules of international law in so far as they are not incompatible with this Part.

Article 79. **Submarine cables and pipelines on the continental shelf.**	1. All States are entitled to lay submarine cables and pipelines on the continental shelf, in accordance with the provisions of this article. 2. Subject to its right to take reasonable measures for the exploration of the continental shelf, the exploitation of its natural resources and the prevention, reduction and control of pollution from pipelines, the coastal State may not impede the laying or maintenance of such cables or pipelines. 3. The delineation of the course for the laying of such pipelines on the continental shelf is subject to the consent of the coastal State. 4. Nothing in this Part affects the right of the coastal State to establish conditions for cables or pipelines entering its territory or territorial sea, or its jurisdiction over cables and pipelines constructed or used in connection with the exploration of its continental shelf or exploitation of its resources or the operations of artificial island, installations and structures under its jurisdiction. 5. When laying submarine cables or pipelines, States shall have due regard to cables or pipelines already in position. In particular, possibilities of repairing existing cables or pipelines shall not be prejudiced.
Article 86. **Application of the provisions of this Part.**	The provisions of this Part apply to all parts of the sea that are not included in the exclusive economic zone, in the territorial sea or in the internal waters of a State, or in the archipelagic waters of an archipelagic State. This article does not entail any abridgement of the freedoms enjoyed by all States in the exclusive economic zone in accordance with article 58.
Article 87. **Freedom of the high seas.**	1. The high seas are open to all States, whether coastal or land-locked. Freedom of the high seas is exercised under the conditions laid down by this Convention and by other rules of international law. It comprises, inter alia, both for coastal and land-locked States: (a) freedom of navigation; (b) freedom of overflight; (c) freedom to lay submarine cables and pipelines, subject to Part IV; (d) freedom to construct artificial islands and other installations permitted under international law, subject to Part IV; (e) freedom of fishing, subject to the conditions laid down in section 2; (f) freedom of scientific research, subject to Parts IV and XIII; 2. These freedoms shall be exercised by all States with due regard for the interests of the States in their exercise of the freedom of the high seas, and also with due regard for the rights under this Convention with respect to activities in the Area.

Article 112. **Right to lay submarine cables and pipelines.**	1. All States are entitled to lay submarine cables and pipelines on the bed of the high seas beyond the continental shelf. 2. Article 79, paragraph 5, applies to such cables and pipelines.
Article 113. **Breaking or injury of a submarine cable or pipeline.**	Every State shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done willfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offence. This provision shall apply also to conduct calculated or likely to result in such breaking or injury. However, it shall not apply to any break or injury caused by persons who acted merely with the legitimate object of saving their lives or their ships, after having taken all necessary precautions to avoid such breaks or injury.
Article 114. **Breaking or injury by owners of a submarine cable or pipeline of another submarine cable or pipeline.**	Every State shall adopt the laws and regulations necessary to provide that, if persons subject to its jurisdiction who are the owners of a submarine cable or pipeline … cause a break in or injury to another cable or pipeline, they shall bear the cost of the repairs.
Article 115. **Indemnity for loss incurred in avoiding injury to a submarine cable or pipeline.**	Every State shall adopt the laws and regulations necessary to ensure that the owners of ships who can prove that they sacrificed an anchor, a net or any other fishing gear, in order to avoid injuring a submarine cable or pipeline, shall be indemnified by the owner of the cable or pipeline, provided that the owner of the ship has taken all reasonable precautionary measures beforehand.
Article 297. **Limitations on applicability of section 2.**	1. Disputes concerning the interpretation or application of this Convention with the regard to the exercise by a coastal State of its sovereign rights or jurisdiction provided for in this Convention shall be subject to the procedures provided for in section 2 in the following cases: (a) when it is alleged that a coastal State has acted in contravention of the provisions of this Convention in regard to the freedom and rights of navigation, overflight or the laying of submarine cables and pipelines, or in regard to other internationally lawful uses of the sea specified in article 58[.]