ARTICLE

UNTWISTING THE SECURITY OF UNDERSEA INTERNET CABLES

David W. Opderbeck[*]

ABSTRACT

The seafloor and its communications infrastructure is a key warfare domain. The global Internet depends on networks of undersea transcontinental cables that are remarkably vulnerable to physical attacks by conventional forces and shadow fleets. Nearly all this infrastructure is privately owned by a small number of providers, including increasingly massive hyperscalers such as Google, Microsoft, and Meta. Responses to incidents that could either be attacks or unfortunate accidents are complicated by questions of intent and attribution as well as by applicable legal frameworks. The law of the sea embedded in the United Nations Convention on the Law of the Sea (UNCLOS) provides some legal touchpoints but these traditional regimes were not designed for the global Internet age. The law of armed conflict (LOAC) applicable to cyberspace as reflected in the Tallinn Manual in key respects is ambiguous concerning cables lying in international waters. This Article examines existing legal frameworks and suggests a multilayered approach that draws on Internet governance bodies, national licensing regimes, open-source monitoring, financial carrots and antitrust sticks, and modifications to UNCLOS, while also warning against some recent policy moves in the United States that would lead to greater fragmentation and less security. Ultimately there is no easy solution to this looming problem. It requires nuanced Internet governance and policy responses and international cooperation.

CONTENTS

---

* Professor of Law and Co-Director, Gibbons Institute of Law, Science & Technology and Institute for Privacy Protection, Seton Hall University School of Law. Thanks to Peter Swire Kevin Frazier, Mailyn Fidler, Asaf Lubin, Gus Hurwitz, and the participants at the 2025 Cybersecurity Law and Policy Scholar's Conference and Law and Technology Workshop for helpful comments on earlier drafts of this paper. Thanks also to Christina Borao for excellent research assistance.

INTRODUCTION

Thirty-three exabytes of data traverse the Internet every day,[1] equal to the contents of fifty-two trillion books.[2] The physical infrastructure supporting these inconceivably vast data flows is also inconceivably vast, comprised of three different tiers of high-bandwidth cables, last mile connections into businesses and homes, private and public networks of every kind, cellular and satellite communications systems, and every device connected to the Internet worldwide, including the laptop on your desk and the phone in your pocket.[3]

About 550 Internet cables connecting the continents and other regions and territories lie under the sea.[4] Compared to all the physical Internet

---

[1] Samir Marwaha, *Sandvine's 2024 Global Internet Phenomena Report: Global Internet Usage Continues to Grow,* APPLOGIC NETWORKS (Apr. 10, 2024), https://www.applogicnetworks.com/blog/sandvines-2024-global-internet-phenomena-report-global-internet-usage-continues-to-grow [https://perma.cc/D3BQ-WLGL]. An exabyte is one quintillion bytes, or a billion gigabytes. Alexander S. Gillis, *Exabyte (EB)*, TECHTARGET (Jan. 31, 2022), https://www.techtarget.com/searchstorage/definition/exabyte [https://perma.cc/BR5Q-VT6R].

[2] *See* Paul Balsom, *The Surprising Things You Don't Know About Big Data*, ADEPTIA (Mar. 5, 2015), https://www.adeptia.com/blog/surprising-things-you-dont-know-about-big-data [https://perma.cc/SB5Y-QT7P] (noting that one exabyte equals 1.6 trillion books).

[3] *See generally* WILLIAM B. NORTON, THE INTERNET PEERING PLAYBOOK (2014); MARTIN WOLSKE, A PERSON-CENTERED GUIDE TO DEMYSTIFYING TECHNOLOGY 59–76 (2d ed. 2023).

[4] *See Submarine Cable Map*, TELEGEOGRAPHY, https://www.submarinecablemap.com/ [https://perma.cc/G93F-CFNV]; *Politics: The Physical Borders of the Digital World*, THE ECONOMIST (Jan. 29, 2024), https://www.economist.com/technology-quarterly/2024/01/29/the-physical-borders-of-the-digital-world [https://perma.cc/DMD6-EXE7].

infrastructure in the world, this is a vanishingly small quantum of cabling. Yet nearly all the intercontinental Internet traffic around the world depends on this relative handful of undersea cables.[5] Without them, the Internet as we know it would not exist. Instead, we might at best experience a disconnected set of terrestrially bound local and national networks, perhaps with some slow and patchy satellite interconnectivity.

Now, it seems these undersea Internet cable choke points are under attack. From 2023 to 2025, numerous Baltic Sea cables connecting Estonia, Finland, Latvia, Sweden, and Germany were damaged, in most cases—it is suspected—by Chinese ships dragging their anchors.[6] In each case the ships claimed no malicious intent, but many observers believe these were intentional acts instigated by Russia in retaliation for the sabotage of the Nordstream undersea gas pipeline in 2022, likely authored by Ukraine.[7] Throughout the war in Ukraine, Russian officials have publicly mused about destroying undersea cables in retaliation for Western sanctions against Russian natural gas.[8] The Russian "shadow fleet" of tankers used to evade oil sanctions has been implicated in numerous cable damage incidents.[9] Between 2023 and 2025, analysts attributed several cable damage incidents to Chinese

---

[5] Media reports frequently assert that 99% of global Internet traffic travels over undersea cables. A measurement with that level of precision is impossible to achieve, but it is undoubtedly true that only a very small fraction travels over the other intercontinental alternative—satellite. *See* Alan Mauldin, *Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?*, TELEGEOGRAPHY BLOG (May 4, 2023), https://blog.telegeography.com/2023-mythbusting-part-3 [https://perma.cc/7CAX-WZVP].

[6] Katharina Bucholz, *Baltic Sea Cable Incidents Pile Up*, STATISTA (Feb. 6, 2025), https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [https://perma.cc/B8SB-CKZP].

[7] *See id.*; Linda Koponen, *The Attack on the Nord Stream Pipelines Was One of the Largest Acts of Sabotage in History. What Really Happened May Be Getting Clearer*, NZZ (Aug. 20, 2024), https://www.nzz.ch/english/the-nord-stream-sabotage-mystery-a-reconstruction-ld.1843733 [https://perma.cc/GNX5-XQZ4].

[8] Mercedes Page, *Could Russia Deliver on its Threat to Cut Subsea Cables?*, THE MARITIME EXECUTIVE (June 25, 2023), https://maritime-executive.com/editorials/could-russia-deliver-on-its-threat-to-cut-subsea-cables [https://perma.cc/7DMP-3HDF].

[9] *See* Rebecca Rosman, *What to Know About Finland, Russia's 'Shadow Fleet' and a Severed Undersea Cable*, NPR (Dec. 31, 2024), https://www.npr.org/2024/12/31/nx-s1-5243302/finland-russia-severed-undersea-cable-shadow-fleet [https://perma.cc/J5RP-CQ59]; Kathryn Diss & Ed Lawrence, *Inside the Mission to Stop Putin's 'Ghost Ships' Wreaking Havoc on the Seas*, ABC NEWS (May 31, 2025), https://www.abc.net.au/news/2025-06-01/inside-mission-to-stop-russian-ghost-ships-cutting-sea-cables/105355746 [https://perma.cc/6BP9-52CQ]; Johanna Lemola & Lynsey Chutel, *Finland Says Vessel Suspected of Cutting Cable May Be Part of Russia's 'Shadow Fleet*', N.Y. TIMES (Dec. 26, 2024), https://www.nytimes.com/2024/12/26/world/europe/finland-estonia-cables-russia.html [https://perma.cc/37EV-LV49].

merchant ships off of Taiwan, again provoking heated disputes about intent in the context of a political tinderbox.[10] One of these incidents involved a ship dragging its anchor while sailing in an unusual zig-zag pattern.[11] In March 2025, four cables were severed in the Red Sea, disrupting about one quarter of the Internet traffic between Asia and Europe.[12] And on September 6, 2025, four major undersea cable systems in the Red Sea that carry traffic to Europe, the Middle East, and Asia were damaged in an anchor-dragging incident, requiring significant re-routing and resulting in substantial data loss in the Middle East.[13]

While questions of attribution and intent linger over recent incidents, there is no doubt that world powers view the seafloor and the communications and energy infrastructure lying on it as a key warfare domain. China, Russia, and the United States, for example, each possess

---

[10] Jamie Ocon & Jonathan Walberg, *China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities*, 10 GLOB. TAIWAN INST. 1, 9 (June 4, 2025); INSIKT GROUP, SUBMARINE CABLES FACE INCREASING THREATS AMID GEOPOLITICAL TENSIONS AND LIMITED REPAIR CAPACITY 11 & Appendix A (July 17, 2025) (identifying at least 44 submarine cable damage incidents from February 2024–June 2025).

[11] INSKIT GROUP, *supra* note 10, at 11.

[12] Antonio Voce, Tural Ahmedzade & Ashley Kirk, *'Shadow Fleets' and Subaquatic Sabotage: Are Europe's Undersea Internet Cables Under Attack?*, THE GUARDIAN (Mar. 5, 2025, last modified July 17, 2025), https://www.theguardian.com/world/ng-interactive/2025/mar/05/shadow-fleets-subaquatic-sabotage-europe-undersea-internet-cables-under-attack [https://perma.cc/76EX-YXNP]; Winston Qui, *PEACE Cable Cut in the Red Sea, Repair to Be Prolonged*, SUBMARINE CABLE NETWORKS (Mar. 7, 2025) https://www.submarinenetworks.com/en/systems/asia-europe-africa/peace/peace-cable-cut-in-the-red-sea%2C-repair-to-be-prolonged [https://perma.cc/3QN6-XJGQ].

[13] *See* Mike Hicks, *Diving Into the Red Sea Cable Cuts & More Outage News*, CISCO THOUSANDEYES (Sept. 19, 2025), https://www.thousandeyes.com/blog/internet-report-red-sea-subsea-cable-cuts [https://perma.cc/D88R-LUDM]; ERIN L. MURPHY & THOMAS BRYJA, CTR. FOR STRATEGIC & INT'L STUD., THE STRATEGIC FUTURE OF SUBSEA CABLES: EGYPT CASE STUDY 1 (2025), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-11/251112_Murphy_Subsea_Cables_Egypt_0.pdf?VersionId=BL1zSd4ltjALOiiP3OyWrr0XX8dv_sRS [https://perma.cc/UWX4-Q4MR]. It is unclear whether any of these anchor-dragging incidents were intentional. The government of Yemen has warned that Houthi rebels have plans to damage cables in the Red Sea, although the recent Red Sea attacks have not been clearly attributed to Houthi activity. *See* Patrick Wintour, *Houthis May Sabotage Western Internet Cables in Red Sea, Yemen Telecoms Firms Warn*, THE GUARDIAN (Feb. 5, 2024) https://www.theguardian.com/world/2024/feb/05/houthis-may-sabotage-western-internet-cables-in-red-sea-yemen-telecoms-firms-warn [https://perma.cc/755T-TSPE]; MURPHY & BRYJA, THE STRATEGIC FUTURE OF SUBSEA CABLES, *supra* note 13, at 6. In one case in the Red Sea in 2024, a ship that was disabled by a Houthi missile damaged cables when dragging its anchor, but this seems an unlikely motivation for the missile strike. *Id.*

specialized submersible vessels capable of attacking undersea cables.[14] These threats add to the ever-growing list of challenges to the utopian dream of the global open Internet.

The bottom of cyberspace is a tangle of routers, modems, switches, repeaters, amplifiers, servers, PCs, laptops, smart phones, and multitudinous Internet of Things (IoT) devices linked by wireless technologies and by good-old-fashioned coaxial and fiberoptic wires.[15] When Senator Ted Stevens described the Internet as a "series of tubes" in 2006, his comments were widely ridiculed, but as technologist Ed Felton noted at the time, Stevens was not entirely wrong.[16] Control over the "tubes" is control over the network. There is no question that the Internet's physical core is vulnerable. And as Asaf Lubin has noted, "every vulnerability is ultimately exploited."[17]

The vulnerability of the Internet's physical core is partly a result of the bottom-up development of Internet governance norms, which are otherwise part of the Internet's transformative genius. In its first thirty or so years, Internet law and policy focused largely on the code and content layers in the domains such as intellectual property, content regulation, and freedoms of speech and association.[18] While scholars and policymakers acknowledged that the physical layer mattered greatly, the default posture in democratic market economies was towards private ownership of most of the Internet's physical infrastructure.[19] This was central to the design of the U.S. Telecommunications Act of 1996, which set the stage for the next thirty years

---

[14] *See* Michael S. Chase, *Capabilities and Implications of China's Jiaolong Submersible*, 10(23) JAMESTOWN: CHINA BRIEF (Nov. 19, 2010), https://jamestown.org/capabilities-and-implications-of-chinas-jiaolong-submersible/ [https://perma.cc/53D5-G9P7]; Peter Suciu, *Russia's Losharik Submarine is Making the Ultimate Comeback*, THE NATIONAL INTEREST (Mar. 18, 2024), https://nationalinterest.org/blog/buzz/russias-losharik-spy-submarine-making-ultimate-comeback-210080 [https://perma.cc/7554-VLNG]; Gabriel Honrada, *New U.S. Spy Sub Built for Seabed War With China*, ASIA TIMES (Apr. 24, 2023), https://asiatimes.com/2023/04/new-us-spy-sub-built-for-seabed-war-with-china/ [https://perma.cc/JZ9L-FGZ5].

[15] *See infra*, Part I.

[16] Ed Felten, *Taking Stevens Seriously*, CITP BLOG (July 17, 2006), https://blog.citp.princeton.edu/2006/07/17/taking-stevens-seriously/ [https://perma.cc/GNV4-DK2S].

[17] Asaf Lubin, *Spying on the Core, in* PROTECTING THE INTERNET'S CORE (MIT Press forthcoming) (on file with author).

[18] *See, e.g.*, LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (Basic Books 2006).

[19] *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (Oxford Univ. Press 2006).

of Internet governance policy.[20] A light regulatory touch encouraged market actors to build out the Internet's physical infrastructure, funded by private capital markets.[21]

With the rise of cloud computing starting in the early-to-mid 2000s, some focus returned to the hardware layer as some states implemented data localization policies, and, separately, disputes arose about civil and criminal process served within a jurisdiction to retrieve records located on servers in other jurisdictions.[22] International human rights scholars and think tanks also began to emphasize how states could engage in censorship by controlling local broadband Internet hubs such as Internet Exchange Points (IXPs).[23] Nevertheless, the hardware layer, when considered at all, was mostly a matter of local concern. While most Internet governance scholars agreed that the code layer should remain open, and that the content layer should enjoy free speech protections and some intellectual property protections, there was little pushback against the fact that most of the hardware layer was privately owned.

The push towards "network neutrality" starting in the early 2000s subtly changed this conversation. While the consensus remained that the code and content layers should remain open and relatively unregulated, many scholars, advocates, and policymakers argued that privately-owned physical backbone infrastructure should be regulated with something like traditional common carrier rules.[24] Backbone providers, argued proponents of network neutrality, should be prohibited from prioritizing or throttling packets relating to any specific edge provider or user.[25] Opponents argued that if consumers demanded neutrality the markets would supply it. The underlying economic question was one of market failure: whether backbone broadband markets were so concentrated that providers would cut self-interested prioritization and throttling deals without much resulting consumer choice.

An often-overlooked spillover of network neutrality was that the regulatory authority for neutrality also provided authority for cybersecurity regulation.[26] Such authority is a doubled-edged sword. It allows regulators to

---

[20] *See* U.S. Telecommunications Act, Pub. L. 104-104, 110 Stat. 56 (1996).
[21] *See infra*, Part I.
[22] *See, e.g.*, CLOUD Act, Pub. L. 115-141, 132 Stat. 1213 (2018) (codified at 18 U.S.C. § 2523 Note).
[23] *See, e.g.*, Loqman Salamatian et al., *The Geopolitics Behind Routes Data Travel: A Case Study of Iran*, 7 J. CYBERSECURITY 1 (2021).
[24] *See infra*, Part I.
[25] *See infra*, Part I.
[26] *See infra*, Part III.B.

enforce uniform basic cybersecurity standards, which should improve the Internet's overall resilience and thereby promote free and open communication at the content layer. But those standards can also entail greater governmental control and surveillance. Since the Obama administration, for instance, U.S. officials have suggested that the President possesses statutory emergency powers to shut down the Internet.[27]

Cybersecurity standards mostly focus on things like software patching, network configuration and traffic monitoring, social engineering training, data governance, incident response, and the like, but they also typically include measures relating to physical security.[28] For example, the NIST Cybersecurity Framework, a widely-recognized process for cybersecurity risk management promulgated by the U.S. National Institute of Standards and Technology, provides that "[a]ccess to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access," asks users to "[a]ssess facilities that house critical computing assets for physical vulnerabilities and resilience issues," and requires monitoring of the physical environment to detect "adverse events."[29]

The NIST Framework is an example of a set of cybersecurity standards that could be entirely voluntary, encouraged by law, or required by law. U.S. law historically has not required backbone providers to implement anything like the NIST Framework at the scale of the physical pipes themselves. While telecommunications law provides regulatory oversight over and permitting requirements for the interconnection of landline telephone and cable television wires, the approach as to broadband Internet cables, including undersea cables, has been mostly hands off.[30]

The one exception to this hands-off approach has been regulation of the landing stations at which undersea cables come on to U.S. soil, going

---

[27] *See* David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 797 (2012); David W. Opderbeck, *Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch?*, 65 FED. COMM. L.J. 1, 3 (2013).

[28] *See, e.g.*, *Cybersecurity Framework 2.0*, NAT'L INST. OF STANDARDS & TECH., COMPUT. SEC. RES. CTR, https://www.nist.gov/cyberframework [https://perma.cc/UV8G-MZZ9].

[29] *NIST Cybersecurity Framework 2.0 Reference Tool*, *ID.RA-01 Ex. 4, PR.AA, DE.CM-02*, NIST COMPUTER SECURITY RESOURCE CENTER, https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters [https://perma.cc/4MMG-AJMN].

[30] *See generally* BROADBAND BRINGING HOME THE BITS 167–215 (Nat'l Academy Press 2002) (ebook), https://www.nationalacademies.org/read/10235/chapter/8 [https://perma.cc/TG78-4AQB].

back to the days of the telegraph.[31] In the version of network neutrality rules adopted by the Biden administration in 2022, this would have changed—the FCC would have taken authority to regulate Internet backbone cybersecurity generally, including network interconnections beyond landing stations. Those network neutrality rules, however, were invalidated by the Sixth Circuit in *Ohio Telecommunications Association v. FCC*.[32]

Meanwhile, international law offers only a minimal framework for the security of undersea cables. The most important treaty, the 1982 United Nations Convention on the Law of the Sea (UNCLOS)—to which the United States is not a signatory—embeds some important principles about the right to lay undersea cables and the duty to avoid damage to cables, but it studiously avoids elements of policing and protection that might cross over into the Law of Armed Conflict (LOAC).[33] LOAC, as interpreted by influential sources on cyber conflict, including the Tallin Manual 2.0, is ambivalent about whether an undersea cable on the high seas could comprise a valid military target and what kind of response is appropriate if a cable is damaged.

The limitations of international law might reflect a need to update principles stemming from Roman times for an age of a global network increasingly used by and for artificial intelligence applications.[34] It might also reflect the tension between the deregulatory Internet exceptionalist ethos of the Telecommunications Act of 1996 and the more realist sensibility of the push for network neutrality regulation.

Consistent with the early utopian vision of a global network unconstrained by the national laws of the "weary giants of flesh and steel," perhaps Westphalian legal structures, including the international law of the sea, are inconsequential to the Internet's continuing vitality and security.[35]

---

[31] *See infra*, Part III.C.

[32] In re MCP No. 185: Ohio Telecomm Ass'n v. FCC, 124 F.4th 993 (6th Cir. 2025). The Sixth Circuit applied the major questions doctrine and held the FCC lacked statutory authority to enact network neutrality rules. *Id.* at 997–98. The litigation resulted from challenges filed by multiple broadband service providers in different districts, and the Judicial Panel on Multidistrict Litigation chose the Sixth Circuit as the forum to hear consolidated petitions for review of the FCC's rule. *Id.* at 1000–01.

[33] U.N. Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994) [hereinafter UNCLOS].

[34] *See infra*, Part I.A.

[35] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/V7EX-H4GS].

Perhaps private property rights and markets can and inevitably will do the heavy lifting, at least against physical undersea disruptions. Maybe the answer is not more regulation but more *redundancy*: that is, more and more cables, built with private equity and protected and repaired out of economic self-interest.[36] But if all this core physical infrastructure is controlled by a handful of powerful private companies, perhaps the *laissez faire* vision is really a dystopia. Should the security and accessibility of global Internet infrastructure belong to Google, Microsoft, Amazon, Meta, and a small group of Tier 1 network providers?

Instead of a sweeping international Internet governance and security regime, or a fully hands-off trust in the bottom-up goodwill of Internet engineers combined with market forces, the best approach may be to strengthen the authority of individual states to police cable damage—for example, by enhanced national cybersecurity requirements connected to territorial landing licenses.[37] The danger with this approach, however, is the prospect of a "splinternet" resulting from divergent security requirements, including arbitrary restrictions on foreign ownership of or investment in cables and cable repair capacity.[38] Russia, China, Iran, Saudi Arabia, and many other states use firewalls, filtering, data localization, government infrastructure control, and other methods to limit their citizens' access to the global Internet.[39] Such efforts contradict the Internet's founding ethos, which is rooted in common standards and global interconnectivity.[40] But in a dizzying reversal, in recent years Russia and China have pushed for greater internationalization of Internet crime enforcement—which includes global

---

[36] *See infra*, Part III.C.
[37] *See infra*, Part III.C.
[38] The term "splinternet" is widely used to describe the results of government Internet control and censorship. *See* Dan York, *What is a Splinternet? And Why You Should be Paying Attention*, INTERNET SOC'Y BLOG (Mar. 23, 2022), https://www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/ [https://perma.cc/T6DG-CANX].
[39] *See generally Key Internet Controls 2024*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2024/key-internet-controls [https://perma.cc/2U2J-Z9MC].
[40] *See, e.g.*, World Summit on the Info. Soc'y, *Declaration of Principles*, ¶ 44, WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003) (stating that "[t]here should be particular emphasis on the development and adoption of international standards. The development and use of open, interoperable, non-discriminatory and demand-driven standards that take into account needs of users and consumers is a basic element for the development and greater diffusion of ICTs and more affordable access to them, particularly in developing countries. International standards aim to create an environment where consumers can access services worldwide regardless of underlying technology.").

surveillance and extraterritorial enforcement authorities—while the United States is enacting ever-tighter restrictions on foreign influence over Internet infrastructure.

These initial reflections suggest this paper's conclusion: the undersea cable security problem requires several measured interventions across international law, national security law, and private law domains. Inaction is unacceptable, but there is no panacea. Part I of this paper describes how undersea cables fit into Internet backbone architecture and discusses the international law of the sea relating to subsea cables, including the strengths and limitations of that law in relation to cable sabotage. Part II discusses other proposals for protecting undersea cables, including cable protection zones, the law of piracy, LOAC, and Chapter VII of the UN Convention. Part III examines whether market provision of redundancy and repair capacity is the most meaningful solution, as compared to the backdrop of cybersecurity provisions in U.S. network neutrality rules and the judicial abrogation of those rules, and ultimately suggests a multilayered suite of tailored legal interventions. Part IV concludes.

I. THE DEVELOPMENT AND VULNERABILITY OF CRITICAL UNDERSEA INTERNET INFRASTRUCTURE

A. Undersea Cables Within the Physical Layer's Ecosystem

The early days of Internet exceptionalism imagined "cyberspace" as a "home of the Mind," free from "weary giants of flesh and steel."[41] It quickly became apparent, however, that "flesh and steel" still very much mattered. The Open Systems Interconnection (OSI) Reference Model, published by the International Organization for Standardization in 1999 identified seven "layers" of internetworking.[42] In the OSI model, the "physical" layer, comprised of electronic circuits, provides the means through which the code and protocols of the data link, network, transport, session, presentation, and application layers flow.[43] Internet law and policy scholars simplified the OSI model into the three layers of hardware, code, and content.[44]

---

[41] Barlow, *supra* note 35.
[42] Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, ISO/IEC 7498-1:1994, *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model* (1994), https://www.iso.org/standard/20269.html [https://perma.cc/3KJB-PBBW].
[43] *Id*.
[44] *See, e.g.*, LESSIG, *supra* note 1918.

When the Internet backbone was privatized starting in the 1990s, a three-tiered structure began to develop organically. Tier 1 Internet service providers operate high bandwidth infrastructure that provides the core "backbone" of the Internet, somewhat analogous to how the Interstate Highway System in the United States functions for container truck traffic.[45] Tier 2 and 3 providers are somewhat analogous to state and county highways in the United States, in that they facilitate traffic to and from the Tier 1 infrastructure as well as carrying some traffic from end to end. In this highway system analogy, think of "end users" as individuals or companies with products in a container that has been picked up by a shipping company at a port and driven over the Interstate Highway System on a large container truck to a warehouse and distribution center somewhere in the interior of the country. At the warehouse and distribution center, the products are sorted and prepared for delivery to the end point by smaller trucks and delivery vans over state and county highways that connect to the Interstate Highway System and from those mid-sized roads to local municipal streets (the "last mile").[46]

End users—the individuals and companies that send and receive data over the Internet—do not ordinarily connect directly to Tier 1 providers. Likewise, edge providers—the entities that provide goods, services, and information over the Internet to end users—usually do not connect directly to Tier 1 providers.[47] End users and edge providers usually connect through "last mile" services offered by Tier 3 providers.[48] Tier 3 providers in turn connect to Tier 2 providers, and Tier 2 providers connect to Tier 1 providers.[49]

These connections between Tier providers can be facilitated through "transit" or "peering" agreements.[50] "Transit" agreements provide access to

---

[45] *See Tier 1 ISPs: A Comprehensive Guide to Global Internet Connectivity*, MACRONET SERVS., (Apr. 24, 2025), https://macronetservices.com/tier-1-isps-a-comprehensive-guide-to-global-internet-connectivity/ [https://perma.cc/W4UR-WA5P].
[46] *See* Phil Yeager, *What Is Intermodal Shipping . . . and Why Should Shippers Care?*, UNION PAC. NEWS (Aug. 4, 2020), https://www.up.com/news/service/tr080420-what-is-intermodal-shipping [https://perma.cc/6VV5-65SC].
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *See* Anindo Mahmood & Murat Yuksel, *Resource Sharing on the Internet: A Comprehensive Survey on ISP Peering*, 57 ACM COMPUT. SURV., Feb. 21, 2025, at 1.

higher Tier providers for a fee.[51] Providers at the same Tier usually can connect settlement-free (i.e., without a fee).[52]

In recent years, "peering" agreements have become more common than transit. "Public peering" arrangements send traffic from multiple networks through Internet Exchange Points (IXPs), usually, but not always, settlement-free.[53] Settlement-free peering can involve non-monetary requirements on providers accessing the IXP, such as network performance, ratio of inbound to outbound traffic, routing policies, and other conditions.[54]

An IXP provides a high-bandwidth hub for traffic into and out of a geographic area.[55] IXPs are most often formed by consortia of ISPs, through public-private partnerships, or by governments. In Europe, the more common model is for IXPs to function as non-profit community-driven organizations with network neutrality requirements.[56] In the United States, IXPs are more commonly for-profit entities, many of which emphasize private peering and "meet me in the room" (MMR) arrangements.[57] In some countries, ISPs are required by law to route through government-controlled IXPs, which facilitates government surveillance, censorship, and Internet shut-downs.[58]

"Private peering" connects two networks together directly.[59] This kind of arrangement can arise when large amounts of data must be shared among discrete nodes on a network or when an enterprise desires more consistent

---

[51] *Id.* at 1–2.
[52] *Id.* at 5.
[53] *Id.* at 15–16; *see also Peering: Understanding Public vs. Private Peering*, GCORE (Jul. 7, 2023), https://gcore.com/learning/understanding-public-vs-private-peering [https://perma.cc/JLH6-7LD6]; *Peering Policy*, CISCO THOUSANDEYES, https://www.thousandeyes.com/learning/techtorials/peering-policy [https://perma.cc/EG5P-DUTE]; Jon Hjembo, *Understanding Peering*, TELEGEOGRAPHY (Nov. 22, 2019), https://blog.telegeography.com/settlement-free-paid-peering-definition [https://perma.cc/Y6VE-Q2QQ].
[54] Mahmoud & Yuksel, *supra* note 50, at 16.
[55] *Internet Exchange Points (IXPs)*, INTERNET SOC'Y, https://www.internetsociety.org/issues/ixps/ [https://perma.cc/49P6-BLP9].
[56] Mahmoud & Yuksel, *supra* note 50, at 9–10.
[57] *Id.* at 10–11. MMR arrangements provide spaces where large ISPs can interconnect.
[58] INTERNET SOC'Y, INTERNET EXCHANGE POINTS: AN INTERNET SOCIETY POLICY BRIEF 3 (2015), https://www.internetsociety.org/wp-content/uploads/2015/10/ISOC-PolicyBrief-IXPs-20151030_nb.pdf [https://perma.cc/Z2EB-QSME]; *Freedom on the Net 2024: Iran*, FREEDOM HOUSE (2024), https://freedomhouse.org/country/iran/freedom-net/2024 [https://perma.cc/J7H7-U244]; *Freedom on the Net 2024: Venezuela*, FREEDOM HOUSE (2024), https://freedomhouse.org/country/venezuela/freedom-net/2023 [https://perma.cc/34R8-36NL].
[59] *Peering: Understanding Public vs. Private Peering*, *supra* note 53.

access speed to cloud services than is available through public peering.[60] Private peering arrangements are available from hyperscale cloud providers contractually for a fee. For example, Microsoft's cloud platform, Microsoft Azure, offers "virtual cloud" private peering options that promise "more reliability, faster speed, and lower latency than typical internet connections."[61]

In addition to backbone providers, IXPs, last mile ISPs, edge providers, and end users, Content Delivery Networks (CDNs) have become crucial to contemporary Internet architecture.[62] CDNs are server networks physically located near last mile networks that cache content from providers such as streaming services so that the content can be delivered more efficiently on demand.[63] CDNs often enter into paid peering arrangements with content providers and last mile ISPs.[64]

Most undersea Internet cables are owned and operated by Tier 1 providers, consortia that include Tier 1 providers, or hyperscalers. Undersea cables come onto shore at cable landing stations (CLSs).[65] CLSs connect to data centers, which in turn connect to the terrestrial Internet stack, whether through IXPs or to other Tier 1 providers through transit arrangements.[66] In other words, in general, undersea cables are part of the Tier 1 physical infrastructure.

---

[60] Paul McGuiness, *When to Use ExpressRoute Local for Microsoft Azure Private Peering*, MEGAPORT (Mar. 15, 2021), https://www.megaport.com/blog/use-expressroute-local-for-azure-private-peering/ [https://perma.cc/64PF-E5UG].
[61] *Azure Express Route*, MICROSOFT, https://azure.microsoft.com/en-us/products/expressroute [https://perma.cc/Q4NU-HLDZ] (last visited Mar. 13, 2026).
[62] Mahmoud & Yuksel, *supra* note 50, at 5.
[63] *Id.*
[64] Examples of well-known CDNs include Akamai, Cloudflare, and Netflix Open Connect.
[65] *See* NANCY ROSS & MAGGIE VENCILL, MITRE, DIGITAL SILK ROAD PEACE SUBSEA CABLE CONNECTIONS TO THE ICT (2024), https://www.mitre.org/sites/default/files/2024-05/PR-24-0996-DSR-Subsea%20Cables.pdf [https://perma.cc/PKZ5-EP4N]; JUSTIN SHERMAN, HOOVER INST., CYBERSECURITY UNDER THE OCEAN: SUBMARINE CABLES AND US NATIONAL SECURITY 2 (2023), https://www.hoover.org/sites/default/files/research/docs/Sherman_CybersecurityUnderOcean_web-rev.pdf [https://perma.cc/TGS4-3335].
[66] ROSS & VENCILL, *supra* note 65.

It costs around $250 million to build an undersea cable between North America and Europe or Asia.[67] In the past, most cables were built by consortia of telecommunications companies, including Tier 1 network providers, that supply bandwidth to Internet service providers and other companies through peering agreements.[68] More recently, cloud hyperscalers, including Google, Amazon, Microsoft, and Meta, have been building out their own undersea networks, both to limit transit or peering fees with traditional network providers and to obtain more control over network availability, bandwidth, and quality. These companies, along with large cloud players such as IBM and Oracle, are often called "hyperscalers" because they provide cloud services at enormous scale.[69]

There are at least three key reasons for this shift. First, each of these hyperscalers also functions as an edge provider. Instead of leasing server space accessed through a Tier 1 ISP, they have built their own massive cloud server infrastructure, including high-bandwidth connections to their server farms. In addition, Amazon, Google, and Microsoft lease their cloud infrastructure to other companies. In fact, together, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform account for over 60% of today's cloud services market.[70] Finally, some of this activity is driven by the rise of artificial intelligence. Large AI models require enormous compute power and large bandwidth. Google and Meta are battling for AI dominance in the United States, in competition with OpenAI, which has had a rocky relationship with Microsoft.[71] The hyperscalers hope building out server and

---

[67] *See* Jonathan Kim, *Subsea Cables: The Invisible Fiber Link Enabling the Internet*, DGTL INFRA (Jan. 16, 2024), https://dgtlinfra.com/submarine-cables-fiber-link-internet/ [https://perma.cc/4BWF-MXC4].

[68] *Id.* One of these, for example, is Lumen Technologies (not to be confused—presumably—with Lumon Industries from the show Severance). Lumen is a Tier 1 provider formerly known as CenturyLink. *Homepage*, LUMEN, https://www.lumen.com/en-us/home.html [https://perma.cc/M9UK-3NQH].

[69] Melissa Palmer, *Hyperscalers: The Complete Guide to What, Why and How*, SOLARWINDS (Jan. 24, 2023), https://www.solarwinds.com/blog/hyperscalers-the-complete-guide [https://perma.cc/N658-NBWH].

[70] Cody Slingerland, *21+ Top Cloud Service Providers Globally in 2025*, CLOUDZERO (May 21, 2025), https://www.cloudzero.com/blog/cloud-service-providers/ [https://perma.cc/6Y8N-GNQD].

[71] *See* KONSTANTIN F. PILZ, YUSUF MAHMOOD & LENNART HEIM, RAND CORP., AI'S POWER REQUIREMENTS UNDER EXPONENTIAL GROWTH (2025), https://www.rand.org/pubs/research_reports/RRA3572-1.html [https://perma.cc/Z7HU-E59R]; Adam Zewe, *Explained: Generative AI's Environmental Impact*, MIT NEWS (Jan. 17, 2025), https://news.mit.edu/2025/explained-generative-ai-environmental-impact-0117 [https://perma.cc/Y5ER-9269]; AUSTIN HORNG-EN WANG & KYLE SILER-EVANS, RAND CORP., U.S.-CHINA COMPETITION FOR ARTIFICIAL INTELLIGENCE MARKETS (2026), https://www.rand.org/pubs/research_reports/RRA4355-1.html [https://perma.cc/WTD4-

bandwidth infrastructure will provide a competitive advantage in emerging AI markets. Not surprisingly, despite significant capital costs and operational risks, the undersea cable market is projected to experience continuing expansion over the next decade.[72]

B. The Existing Legal Mosaic

1. Traditional Law of the Sea: Brief Background

The law of the sea can be understood as one of the first fruits of modernity.[73] Roman law identified the seas as the common possession of all people, borrowing from earlier norms in Greece and the ancient near east.[74] At the same time, the Romans also referred colloquially to the Mediterranean Sea as *"mare nostrum"* ("our sea") and declared it *"mare clausum*" ("closed sea") during the winter months when navigation was difficult. Long-established practice therefore held that everyone was free to use the seas for transportation and trade but also that governing authorities, at least along the coasts, could declare the seas "closed."

The "discovery" of the new world by Columbus in 1492—one marker of the transition from the Middle Ages to modernity—intensified the rivalry between Europe's major sea powers, Spain and Portugal. The Papal Bull *Inter Caetera* in 1493 assigned to Spain all lands west of a demarcation line one hundred leagues west of the Azores and Cape Verde Islands.[75] The pernicious doctrine of discovery, which authorized European colonization of the Caribbean and North and South America, thereby also established the

---

QVAY]; Tech-Explorer, *OpenAI vs. Google vs. Meta: Who Will Win the AI Race in 2026?*, MEDIUM (Dec. 4, 2025), https://medium.com/@techyman/openai-vs-google-vs-meta-who-will-win-the-ai-race-in-2026-5068e08bd7ae [https://perma.cc/X3W3-R29C].

[72] *Submarine Cable System Market Set to Reach $30.50 Billion by 2030, Driven by Growing Data Demand*, NEXGEN NETWORKS (Sept. 24, 2024), https://www.nexgen-net.com/post/submarine-cable-system-market-set-to-reach-30-50-billion-by-2030-driven-by-growing-data-demand [https://perma.cc/4ZDC-S7AK].

[73] *See* M.C.W. Pinto, *Hugo Grotius and the Law of the Sea*, *in* LAW OF THE SEA, FROM GROTIUS TO THE INTERNATIONAL TRIBUNAL FOR THE LAW OF THE SEA 18-47 (Lilian del Castillo ed., 2015); Tullio Scovazzi, *The Origin of the Theory of Sovereignty of the Sea*, *in* LAW OF THE SEA, *supra* note 73, at 48–63.

[74] *See* DOUGLAS M. JOHNSTON, THE THEORY AND HISTORY OF OCEAN BOUNDARY-MAKING 44–45 (1st ed. 1988).

[75] POPE ALEXANDER VI, INTER CAETERA (1493) https://www.papalencyclicals.net/alex06/alex06inter.htm [https://perma.cc/4CRT-Y9YG].

principle that an internationally binding norm could regulate passage over the open seas.[76]

Inter Caetera, in fact, was not without precedent. The Byzantine *Lex Rhodia* concerned Mediterranean trade in the 6th to 8th centuries CE.[77] And the bull *Romanus Pontifex* in 1455 had granted the Portuguese any lands south of Cape Bojador in Africa (located at the western edge of the present-day Western Sahara territory).[78] But *Inter Caetera* was the first instrument purporting to establish jurisdiction on what we now consider the global seas.

The question of sea passage became more fraught with the rise of chartered trading companies in the early 17th century. The seizure of the Portuguese carrack *Santa Catarina* by Dutch East India Trading Company ships off the coast of Singapore in 1603 touched off a legal dispute that boiled over into the Dutch-Portuguese War.[79] The Portuguese claimed that the principle of *mare clausum* (closed sea) gave them control over the Singapore trade.[80] The Dutch, represented by Hugo Grotius, argued for a more ancient principle of *mare liberum* (open sea), resulting in one of Grotius' major works of the same name.[81] The legal debate was joined by English jurist John Selden, who argued for *mare clausum* as the ancient natural law principle in a book by that name.[82]

---

[76] *See* Travis Tomchuk, *The Doctrine of Discovery*, CANADIAN MUSEUM FOR HUM. RTS. (Nov. 2, 2022), https://humanrights.ca/story/doctrine-discovery [https://perma.cc/L7Y7-P8CS]. American courts seized on this history as part of the rationale for American dispossession of native peoples. *See, e.g.*, State v. Foreman*,* 16 Tenn. 256, 258–268 (1835) (stating that "[o]ur [white European] rights on this continent had their origin in discovery in the fifteenth century" and referring to *Inter Caetera* against claims of native sovereignty); BENJAMIN STRAUMANN, ROMAN LAW IN THE STATE OF NATURE: THE CLASSICAL FOUNDATIONS OF GROTIUS' NATURAL LAW 28 (1st ed. 2015). In 2023, the Catholic Church disavowed the doctrine of discovery. *Joint Statement of the Dicasteries for Culture and Education and for Promoting Integral Human Development on the "Doctrine of Discovery"*, HOLY SEE PRESS OFF. (Mar. 30, 2023), https://press.vatican.va/content/salastampa/en/bollettino/pubblico/2023/03/30/230330b.html [https://perma.cc/VX3Q-T97Y].

[77] *See* Alexander Kazhdan, *Lex Rhodia*, *in* THE OXFORD DICTIONARY OF BYZANTIUM (2005).

[78] *See* POPE NICHOLAS V, ROMANUS PONTIFEX (Jan. 8, 1455), https://www.papalencyclicals.net/nichol05/romanus-pontifex.htm [https://perma.cc/8Y4U-XEBZ]. The doctrine of discovery inherent in *Romanus Pontifex* also was disavowed by the Catholic Church in 2023. *Joint Statement on the "Doctrine of Discovery"*, *supra* note 76, at 15.

[79] *See* Jeroen Vervliet, *General Introduction in* HUGO GROTIUS MARE LIBERUM 1609–2009, at ix, ix–xxviii (Robert Feenstra ed., 2009).

[80] *See id*.

[81] *See id.*

[82] *See id.*

Grotius' position eventually won the day, with a compromise crafted by Cornelius Bynkershoek in *De Dominium Maris*: a nation could control the waters within cannon shot of its shoreline.[83] The law of *mare liberum* coupled with the cannon-shot rule supplied the principle that still applies in international law today. The open seas—in today's legal terminology, "international waters"—are open to free passage regardless of nationality, while a state has the right to control the waters within some measurable distance of its shoreline.

Mare liberum, qualified by the cannon-shot rule, did not address related problems of privateering, prize-taking, piracy, and the slave trade.[84] These questions were addressed primarily under the then-developing international law of war. Under this nascent international law, *mare liberum* did not prohibit states from engaging with hostile armed forces in international waters in times of war. To the contrary, warships were even granted rights against interference by neutral states. Further, the practice of issuing letters of marque enabled states to commission otherwise civilian ships within their war-fighting fleets and thereby authorized the practices of privateering and prize-taking.[85]

The Slave Trade Acts of 1807 passed by the British Parliament and the U.S. Congress banned the trans-Atlantic slave trade and authorized the two nations to enforce the ban against ships sailing under their own national flags.[86] The British enforced the ban robustly through its West Africa Squadron.[87] The United States attempted only spotty enforcement before the Civil War. Treaties between Britain and Spain, the Netherlands, Sweden, Brazil, Madagascar, France, Denmark, various North African territories, and South American countries signed from 1822 through the later 19th century authorized the Royal Navy to seize slaving ships controlled by nationals of

---

[83] *See id.*
[84] *See id.*
[85] *See* STEVE P. MULLIGAN, CONG. RSCH. SERV., LSB11272, LETTERS OF MARQUE AND REPRISAL (PART 1): INTRODUCTION AND HISTORICAL CONTEXT (2025), https://www.congress.gov/crs-product/LSB11272 [https://perma.cc/5EK5-C9H3].
[86] Slave Trade Act 1807, 47 Geo. 3 c. 36 (UK); An Act to Prohibit the Important of Slaves, ch. 22, § 1, 2 Stat. 426 (1807).
[87] *See generally* MARY WILLS, ENVOYS OF ABOLITION: BRITISH NAVAL OFFICERS AND THE CAMPAIGN AGAINST THE SLAVE TRADE IN WEST AFRICA (2019); CHRISTOPHER LLOYD, THE NAVY AND THE SLAVE TRADE: THE SUPPRESSION OF THE AFRICAN SLAVE TRADE IN THE NINETEENTH CENTURY (1949); WILLIAM WARD, THE ROYAL NAVY AND THE SLAVERS: THE SUPPRESSION OF THE ATLANTIC SLAVE TRADE (1969).

signatory countries.[88] There is thus significant precedent for agreement between states for the use of military force to police certain kinds of conduct in territorial and international waters.

2. The 1884 Cable Convention

The late 19th century saw the rise of a technological innovation that transformed human communication and raised questions under the traditional law of the sea: the telegraph. The first trans-oceanic telegraph cable was laid in 1858, culminating in a message between Queen Victoria and U.S. President James Buchanan.[89] Under the existing law of the sea, states and private parties flying under a flag had rights of passage through international waters. These rights were presumed to allow cable-laying, but states could only protect cables and cable-laying ships in their territorial waters. The 1884 Cable Convention, which applied outside territorial waters, made it:

> [A] punishable offence to break or injure a submarine cable, wilfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communication, either wholly or partially, such punishment being without prejudice to any civil action for damages.[90]

The Convention required cable-laying ships to display unique signals and required other ships to stay at least one nautical mile away from ships bearing cable-laying signals.[91] There were exceptions to these rules for emergencies and provision for recompense if a ship sacrificed an anchor, net,

---

[88] *See* Treaty for the Abolition of the Slave Trade, Gr. Brit.-Spain, Sept. 23, 1817, 67 C.T.S. 397; Treaty of The Hague, Gr. Brit.-Neth., May 4, 1818, 68 C.T.S. 445; Treaty of Stockholm, Gr. Brit.-Swed., Mar. 3, 1813, 62 C.T.S. 175; Convention for the Abolition of the African Slave Trade, Gr. Brit.-Braz., Nov. 23, 1826, 76 C.T.S. 427; Treaty for the Abolition of the Slave Trade, Gr. Brit.-Madag., Oct. 23, 1817, 68 C.T.S. 115; Treaty for the Suppression of the African Slave Trade, Gr. Brit.-Fr., Dec. 20, 1841, 92 C.T.S. 437; Treaty of Kiel, Gr. Brit.-Den., Jan. 14, 1814, 63 C.T.S. 297; General Treaty, Gr. Brit.-Morocco, Dec. 9, 1856, 116 C.T.S. 121; Treaty of Peace and Commerce, Gr. Brit.-Tripoli, Apr. 29, 1816, 66 C.T.S. 43; Treaty of Peace and Commerce (Renewed), Gr. Brit.-Algiers, Aug. 28, 1816, 66 C.T.S. 245; Treaty of Amity, Commerce, and Navigation, Gr. Brit.-Colom., Apr. 18, 1825, 75 C.T.S. 195. Prior to the Civil War, the U.S. did not join these treaties.

[89] Allison Marsh, *The First Transatlantic Cable Was a Bold, Beautiful Failure*, IEEE SPECTRUM (Oct. 31, 2019), https://spectrum.ieee.org/the-first-transatlantic-telegraph-cable-was-a-bold-beautiful-failure [https://perma.cc/7BH5-ZVXM]. The message took nearly sixteen hours to traverse the cable. *Id.*

[90] Convention for the Protection of Submarine Telegraph Cables arts. I, II, Mar. 14, 1884, 24 Stat. 989.

[91] *Id.* art. V.

or fishing gear to avoid damaging a cable.[92] The Convention did not suggest violation of its terms was an act of war, but rather enabled member states to enact domestic measures for criminal enforcement.[93]

3. Current International Law

The most comprehensive current source of positive international law concerning the law of the sea is UNCLOS. The People's Republic of China and the Russian Federation have ratified UNCLOS. Despite efforts under several presidents, the United States has not ratified.[94]

UNCLOS preserves and extends the customary international law framework. Under UNCLOS, states retain full jurisdiction over territorial waters within 12 nautical miles (nm) of the coastline.[95] In addition to the 12nm line, UNCLOS provides for a Contiguous Zone extending 24nm from the coast and for an Exclusive Economic Zone (EEZ) extending up to 200 nautical miles from the coast.[96] Within the Contiguous Zone, states may enforce their customs, fiscal, immigration, or sanitary laws.[97] Within an EEZ, states have sovereign rights over marine exploration, natural resources, artificial islands, and other installations.[98] Finally, states have rights to exploration and natural resources extending to their continental shelf, which "comprises the seabed and subsoil of the submarine areas that extend beyond its territorial sea throughout the natural prolongation of its land territory to

---

[92] *Id.* arts. II, VII.
[93] *Id.* arts. VIII–XII.
[94] UNCLOS, *supra* note 33; *see UNCLOS List of Ratifying Parties*, U.N. TREATY COLLECTION, https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=en [https://perma.cc/AM3Q-FN2J]; *Should the United States Ratify the Law of the Sea?*, COUNCIL ON FOREIGN RELS. (July 3, 2024), https://education.cfr.org/teach/mini-simulation/should-united-states-ratify-law-sea [https://perma.cc/4R5Z-GC2Z]; Will Shrepferman, *Hypocri-sea: The United States' Failure to Join the UN Convention on the Law of the Sea*, HARV. INT'L REV. (Oct. 31, 2019), https://hir.harvard.edu/hypocri-sea-the-united-states-failure-to-join-the-un-convention-on-the-law-of-the-sea-2/ [https://perma.cc/2WS4-WPKV].
[95] UNCLOS, *supra* note 33, art. 3.
[96] *Id.* art. 33.
[97] *Id.* art. 33(1).
[98] *Id.* art. 56.

the outer edge of the continental margin," up to a distance of 200nm from the baseline or beyond based on certain stated measurements.[99]

The high seas "are open to all States" and entail the right of freedom of navigation.[100] The high seas are used only "for peaceful purposes" and cannot validly be subjected to any state's sovereignty.[101] Ships of all states enjoy rights of "transit passage" through straits used for international navigation between different parts of the high seas or EEZs.[102] In addition, ships of all states enjoy rights of "innocent passage" through the territorial seas of other states.[103] Article 19 states that "[p]assage is innocent so long as it is not prejudicial to the peace, good order or security of the coastal State."[104]

UNCLOS also regulates cable-laying activities and the protection of undersea cables. Article 112 states that "[a]ll States are entitled to lay submarine cables and pipelines on the bed of the high seas beyond the continental shelf."[105] Article 113 requires states to adopt laws penalizing breaking or injuring a submarine cable or pipeline "done wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications" except in cases of emergency.[106] Article 115 requires states to adopt laws granting compensation to owners of ships that have sacrificed an anchor, net or other fishing gear to avoid injury to a submarine cable.[107] States also have the right to lay submarine cables and pipelines on the continental shelf and to control cables or pipelines entering their territorial seas.[108]

Nothing in these provisions explicitly authorizes a state to patrol the high seas to protect undersea cables. Two provisions, however, could provide some leeway. First, a warship on the high seas is immune from the jurisdiction of any state other than the state of its flag, as are ships "owned or operated by a State and used only on government non-commercial

---

[99] *Id.* art. 76. The baseline may vary depending on the nature of the coast. *See id.* arts. 5 (normal baseline), 6 (reefs), 7 (straight baseline), 9 (river mouths), 10 (bays), 13 (low-tide elevations), 47 (archipelagic states).
[100] *Id.* arts. 86–87.
[101] *Id.* art. 88.
[102] *Id.* arts. 37–39.
[103] *Id.* art. 19.
[104] *Id.* art. 19.
[105] *Id.* art. 112.
[106] *Id*. art. 113.
[107] *Id.* art. 115.
[108] *Id.* art. 79.

service."[109] This reflects the fact that UNCLOS concerns ordinary navigation for commerce, travel, migration, and research, while the operation of warships on the high seas is governed by the international law of war. A warship, then, presumably could interdict a ship sabotaging undersea cables if that action is consistent with the laws of war. It is unclear, however, whether an act of cable sabotage would comprise an act of war warranting such a response, even if the act could be attributed to a state actor under the laws of war.[110]

In addition, Article 100 places a duty on all states to repress piracy and Article 105 allows any state to seize a pirate ship on the high seas, to arrest the persons on board, and to confiscate the ship's property.[111] If sabotage of undersea cables were an act of piracy, then such a seizure could be valid even if the sabotage did not constitute an act of war. As discussed in Part II, *infra*, however, the UNCLOS definition of piracy makes this approach legally dubious.

II. PROPOSALS UNDER INTERNATIONAL LAW

In recent years, scholars and policymakers have advanced several proposals aimed at providing more protection for undersea cables, including cable protection zones, authorizations for states to use force against sabotage as acts of piracy, considering cable sabotage an act of war, and a new international convention specific to undersea cables.[112]

Of course, as a practical matter, even absent any of these international law provisions, a state with sufficient resources could use naval assets to seize ships suspected of cable cutting on the high seas or anywhere else in the world without real consequences. The United States's actions in seizing ships involved with Venezuelan oil transport after the U.S. military ouster of President Nicolás Maduro, and the U.S. destruction of ships allegedly

---

[109] *Id.* art. 95–96.
[110] *See infra*, Part II.D.
[111] *Id.* arts. 100, 105.
[112] *See* Thea Coventry, *What Should States Do to Combat the Sabotage of Submarine Cables and Pipelines Beneath the High Seas/EEZs?* EJIL: TALK! (Dec. 13, 2024), https://www.ejiltalk.org/what-should-states-do-to-combat-the-sabotage-of-submarine-cables-and-pipelines-beneath-the-high-seas-eezs/ [https://perma.cc/J5DJ-XREH].

engaged in drug trafficking in the Caribbean, demonstrate this reality.[113] Few observers who care about international law would condone this approach.[114]

International relations scholars in the realist school might argue that these facts about power on the ground (or on the waves) demonstrate that international law does not, in the end, matter very much.[115] A discussion of the debate between international law legalists and realists is far beyond the scope of this paper. We can note, however, that this debate becomes particularly challenging when applied to the inherently bottom-up, democratic, and transnational ideals of Internet governance.[116] This challenge is even more acute in an era when current United States leadership is aggressively undermining the rules-based international order created after World War II in ways that undermine the assumptions of international relations realists and legalists alike.[117] An emphasis on the content of

---

[113] *See America Chases Down the Shadow Fleet Serving Venezuela,* ECONOMIST (Jan. 7, 2026), https://www.economist.com/briefing/2026/01/07/america-chases-down-the-shadow-fleet-serving-venezuela [https://perma.cc/B543-QETA]; Max Bearak, Simón Posada, & Christian Triebert, *Grim Evidence of Trump's Airstrikes Washes Ashore on a Colombian Peninsula*, N.Y. TIMES (Dec. 29, 2025), https://www.nytimes.com/2025/12/29/world/americas/trump-boat-strikes-gulf-of-venezuela-wreckage.html [https://perma.cc/HT3C-NYEL].

[114] *See, e.g.*, Charlie Trumbull, *The Administration's Drug Boat Strikes Are Crimes Against Humanity*, LAWFARE (Dec. 16, 2025), https://www.lawfaremedia.org/article/the-administration-s-drug-boat-strikes-are-crimes-against-humanity [https://perma.cc/V5WB-YLVL]; Gabor Rona, *Venezuelan Boat Attacks: Utterly Unprecedented and Patently Predictable*, LAWFARE (Oct. 2, 2025), https://www.lawfaremedia.org/article/venezuelan-boat-attacks--utterly-unprecedented-and-patently-predictable [https://perma.cc/7VUQ-8A7K].

[115] For a discussion of the broader debate between international law and realist international relations scholars, see, e.g., *Symposium Debate Transcript: The Promise of International Law: Realism versus Legalism*, 11 NOTRE DAME J. INT'L & COMP. L. 91 (2021); Daniel Abebe, *Why Comparative International Law Needs International Relations Theory*, *in* COMPARATIVE INTERNATIONAL LAW 71–88 (2018); Ryan Mitchell, *Sovereignty and Normative Conflict: International Legal Realism as a Theory of Uncertainty*, 58 HARV. J. INT'L L. 421 (2017).

[116] *See* WORLD SUMMIT ON THE INFORMATION SOCIETY DECLARATION OF PRINCIPLES (Dec. 12, 2003), https://www.itu.int/net/wsis/docs/geneva/official/dop.html [https://perma.cc/F95X-FSLA]; John Mathiason, *Internet Governance Wars: The Realists Strike Back*, 9 INT'L STUD. REV. 152 (2007) (reviewing JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (Oxford Univ. Press 2006)); Charles W. Kegley, Jr., *Realism in the Age of Cyber Warfare*, J. OF CARNEGIE COUNCIL FOR ETHICS & INT'L AFF. (Apr. 26, 2021), https://www.ethicsandinternationalaffairs.org/online-exclusives/realism-in-the-age-of-cyber-warfare [https://perma.cc/4C7S-WLW3].

[117] *See, e.g.*, Daniel W. Drezner & Elizabeth N. Saunders, *Trump's Year of Anarchy: The Unconstrained Presidency and the End of American Primacy*, FOREIGN AFF. (Jan. 20, 2026), https://www.foreignaffairs.com/united-states/trumps-year-anarchy/ [https://perma.cc/ZM7N-JHGM]. As Drezner and Saunders argue, the world Trump is creating is not the anarchy that

international law at least highlights norms that could shape discourse about the actions of the great and once-great powers, including the United States, China, and Russia, as they fight for dominance over cyberspace. As the following subsections demonstrate, however, the existing applicable international law proves inadequate even on its own terms.

A. Cable Protection Zones

Some countries that are parties to UNCLOS, including Australia, New Zealand, Japan, and Singapore, have created submarine cable protection zones that go beyond UNCLOS to restrict activities such as fishing, dredging, mining, and anchoring in designated areas.[118] Violations are subject to civil or criminal penalties enforced by the state that created the zone.[119]

It is unclear whether such unilaterally enacted cable protection zones are consistent with international law if they extend beyond a state's territorial sea.[120] Since UNCLOS recognizes that states may possess some rights to manage traffic and resources beyond the territorial sea, through the creation of EEZs and through control of resources on the continental shelf, the creation of a cable protection zone that extends into an EEZ or to the continental shelf might find support in existing norms.[121] A cable protection zone that extended into the high seas, however, would seem to violate the norm leaving the high seas open to all.[122]

Even if cable protection zones are consistent with international law in territorial, EEZ, or continental shelf waters, they cannot change international law relating to the *enforcement* of criminal laws. Under existing international law, a state can only enforce criminal sabotage laws against its own flag vessel or foreign individuals within its territory, with limited exceptions

---

contemporary realists write about, in which states must make prudent choices about when and where to act, with whom and against whom to ally, and how and how much to impose their will on others. In that world, order remains possible. Trump, by contrast, makes critical decisions with little to no process at seemingly random times—unprompted by emergencies. By seizing the tools of hegemony, Trump is acting aggressively in multiple regions at the same time, at a speed that no previous great power could contemplate.

[118] *Id*.

[119] *Id.*

[120] *See* Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations r. 54, ¶ 14, at 256 (Michael N. Schmitt, 2d ed., 2017).

[121] *See id.*

[122] *Id.*

relating to piracy and the slave trade.[123] Only the state of the ship's flag possesses enforcement jurisdiction over ships in an EEZ or on the high seas.[124] In other words, cable protection zones are legally unenforceable by the legislating state outside its territorial waters except against ships under the flag of the legislating state. To become more broadly effective, groups of neighboring states would need to adopt multilateral reciprocity rules, and states known for offering flags of convenience would also need to get on board.[125]

1. Cable Sabotage as an Act of Piracy

As noted in Part I, *supra*, Article 100 of UNCLOS places a duty on all states to repress piracy, and Article 105 allows any state to seize a pirate ship on the high seas and to arrest the persons on board and confiscate its property.[126] A "pirate ship" is defined as one intended to be used for the purpose of

> (a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
>
> (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
>
> (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State. . . .[127]

This has been called the "two-vessel" rule: piracy occurs only when one ship or its passengers directs certain acts against another ship or its passengers or property.[128] An undersea cable obviously is not a ship or

---

[123] *See* Robert Beckman, *Protecting Submarine Cables from Intentional Damage—the Security Gap*, *in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 284–85 (Douglas Burnett et al. eds., 2014).
[124] *Id*.
[125] *See* Anna Fleck, *Flags of Convenience Dominate Maritime Freight*, STATISTA (Jan. 11, 2023), https://www.statista.com/chart/29086/flags-of-convenience/ [https://perma.cc/PG79-2HWD].
[126] UNCLOS, *supra* note 33, art. 105.
[127] *Id*. arts. 101, 103.
[128] Mick P. Green & Douglas R. Burnett, *Security of International Submarine Cable Infrastructure: Time to Rethink? in* LEGAL CHALLENGES IN MARITIME SECURITY 557, 575–76 (Myron H. Nordquist et al. eds., 2008).

aircraft, so acts of cable sabotage do not fall literally within the two-ship rule and a ship facilitating such acts is not a "pirate ship." The second part of the definition, however, complicates the interpretation and application of this provision to undersea cables. Perhaps undersea cables are property and the deep seabed of the open seas is "outside the jurisdiction of any State."[129]

In fact, Mick Green and Douglas Burnett have argued that the two-vessel rule is not part of the UNCLOS definition of piracy.[130] They suggest that the second part of the definition refers to property other than that which is "on board" a targeted ship as specified in the first part of the definition.[131] In conjunction with a broad rule of construction and evidence of prior practice, they argue that the UNCLOS definition therefore covers undersea cables as a kind of "property."[132] Other commentators have noted that this "creative" interpretation is unlikely to be recognized because states have interpreted the concept of "piracy" narrowly in other contexts involving serious crimes, including relating to terrorism.[133]

The difference, if any, between sub-parts (i) and (ii) is hard to determine: if sub-part (i) already covers ships and aircraft on the high seas, and the high seas are not subject to the jurisdiction of any state, why does sub-part (ii) also refer to ships and aircraft? It appears the drafters had in mind the same type of offense in two different places: the high seas, and some other type of place outside any state's jurisdiction. In fact, the distinction was introduced in the 1958 Geneva Convention on the High Seas (from which the UNCLOS definition is derived) to cover acts "committed by a ship . . . [against persons or property] on an island constituting *terra nullius* or on the shores of an unoccupied territory."[134]

---

[129] *Id.* at 581.
[130] *See id.* at 578; *see also* Douglas Guilfoyle, Tasmin Phillipa Paige, & Rob McLaughlin, *The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables*, 71 INT'L & COMPAR. L. Q. 657, 670–71 (2022).
[131] Green & Burnett, *supra* note 128, at 578.
[132] *Id.* at 578–79.
[133] *See* Beckman, *supra* note 123, at 289.
[134] ILC, REPORT OF THE INTERNATIONAL LAW COMMISSION: COMMENTARIES TO THE ARTICLES CONCERNING THE LAW OF THE SEA, UN Doc A/3159 (1956), GAOR 11th Sess. Suppl. 9, 12, 28 (Art. 39); *see also* Guilfoyle, Page & McLaughlin, *supra* note 130130, at 671 (arguing that this suggests a *broader* reading of sub-part (ii) where there is property not connected to a ship on the high seas, but it seems a stretch to analogize a buried marine cable to an island that is *terra nullius*).

Green and Burnett's textualist reading against a strict two-ship rule, then, appears to ignore drafting history and state practice that suggest that the second part of the definition applies only to "persons or property" on *terra nullius*. *Terra nullius* is unclaimed land that can be lawfully appropriated.[135] The seabed has not been defined in international law as *terra nullius*. Under UNCLOS, the seabed is designated as "the common heritage of mankind" and therefore not subject to any claim of sovereignty.[136] The right to lay cables and pipelines and conduct mining activities on the seabed reflects the seabed's status as a global commons and the right to control aspects of the continental shelf is a unique extension of sovereignty in UNCLOS.[137]

In any event, even if the definition of piracy extended to acts against submarine cables, the "for private ends" condition in the definition reflects the customary international law principle that a governmental vessel or warship's activities cannot be defined as piracy unless the crew has mutinied.[138] The definition therefore would not cover sabotage of submarine cables by state actors. If action against "piracy" is to mitigate some of the threats to undersea cables, an amendment to UNCLOS will be necessary.

2. Cable Sabotage as a "Threat to the Peace"

The "piracy" provisions in UNCLOS and customary international law establish specific and limited reasons for state action against private vessels on the high seas. Even if cable-damaging activity does not fit the definition of "piracy," some scholars have argued, general provisions concerning threats to peace in Article 39 of the U.N. Charter might provide a broader avenue for engagement. [139] The political difficulties underlying Article 39 and the piecemeal nature of attacks on submarine cables, however, limit the utility of this possible avenue.

Article 39 of the U.N. Charter empowers the U.N. Security Council to "determine the existence of any threat to the peace, breach of the peace, or act of aggression" and to take further action in response to such circumstances.[140] Such further action can include economic sanctions,

---

[135] Green & Burnett, *supra* note 128, at 671; *see also* Petra Gumplová, *Justice on the Seafloor: A Critical Appraisal of the Extension of Sovereign Rights to Natural Resources on the Continental Shelf*, 26 GERMAN L. J. 636, 640 (2025).
[136] UNCLOS, *supra* note 33, arts. 136–37.
[137] *Id.* arts. 76–85; *see* Gumplová, *supra* note 135, at 641–44 (discussing the innovation in UNCLOS of extending a kind of sovereignty over the continental shelf).
[138] UNCLOS, *supra* note 33, art. 101.
[139] *See* Guilfoyle, Paige & McLaughlin, *supra* note 130, at 676–79.
[140] U.N. Charter art. 39.

"complete or partial disruption of . . . rail, sea, air postal, telegraphic, radio, and other means of communication," and the use of military force.[141] Critics have argued that the Security Council's actions under Article 39 have been arbitrary, inconsistent, and sometimes nakedly political.[142] These concerns suggest that the Article 39 process would not prove effective against cable sabotage. This is particularly salient because Russia and China, the most prominent suspects in state-sponsored cable-cutting, are permanent members of the Security Council.[143]

Others have suggested that there is at least a pattern of gravity reflected in the Security Council's decisions.[144] The range of circumstances the Security Council has identified under Article 39 includes "country-specific situations such as inter- or intra-state conflicts or internal conflicts with a regional or sub-regional dimension" and "potential or generic threats as threats to international peace and security, such as terrorist acts, the proliferation of weapons of mass destruction or the proliferation and illicit trafficking of small arms and light weapons."[145] For example, in its most recent report on Article 39 activities, the Security Council "reaffirmed that the situations in Afghanistan, the Central African Republic, the Democratic Republic of the Congo, Haiti, Lebanon, Libya, Mali, Somalia, South Sudan and the Sudan (including Abyei), Yemen and the former Yugoslavia constituted threats to regional and/or international peace and security," discussed drug trafficking in Afghanistan, addressed nuclear and biological weapons proliferation in North Korea, the Al-Shabaab terrorist group in Somalia, and reported on a high-level consultation on artificial intelligence.[146]

Given this history, Douglas Guilfoyle, Tasmin Phillipa Paige, and Rob McLaughlin suggest that cable sabotage could satisfy Article 39 because "the potential scale of harm to a State, or group of States, resulting from the severing of a submarine cable is potentially catastrophic, affecting almost all

---

[141] *Id.* arts. 40–42.
[142] *See* Guilfoyle, Paige & McLaughlin, *supra* note 130, at 676–77.
[143] *See* U.N. Sec. Council, *Current Members*, https://main.un.org/securitycouncil/en/content/current-members# [https://perma.cc/454G-XDZ3] (last visited Apr. 6, 2026).
[144] *See* Guilfoyle, Paige & McLaughlin, *supra* note 130, at 677.
[145] U.N. Sec. Council, *Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*, https://main.un.org/securitycouncil/en/content/repertoire/actions [https://perma.cc/WE42-DDA8] (last visited Apr. 6, 2026).
[146] Rep. of the Practice of the S.C., at 479, U.N. Doc. ST/PSCA/1/Add.26 (2023).

aspects of national life. . . ."[147] This might be accurate as to some states that are only connected by one or a very small number of cables, but it is an overstatement as to larger states that might be inconvenienced but not gravely affected by an attack on a single cable. It therefore seems unlikely that relatively isolated acts of Internet cable-cutting would rise to the level of threat that has previously been noticed by the Security Council under Article 39. Article 39 might be a better fit if there was a sustained, coordinated attack on multiple cables, which could produce more dire consequences even in regions with more connection pathways. An attack of that scale, however, could likely only be perpetrated by China, Russia, or the United States, each of which holds veto power over any Security Council Action.[148] Article 39 therefore seems an unlikely vehicle for undersea cable security.

3. Cable Sabotage and the Law of Armed Conflict

UNCLOS sets out the law of the sea during peacetime. It encodes the customary international law principle that a nation's warships enjoy free passage over the high seas, but it does not address the law of the sea during wartime, which is instead governed by the international law of armed conflict (LOAC). LOAC includes principles governing the start of armed conflict (*jus ad bellum*) and conduct within armed conflict (*jus in bello*).[149]

Jus ad bellum principles prohibit armed attacks except for defensive purposes, arguably including preemptive defense.[150] An action by a state to cut or damage Internet cables connecting another state, absent a legitimate defensive justification, could be considered an unlawful act of war. Core *jus in bello* principles include the related requirements of discrimination and proportionality.[151] Only people, institutions, and materiel engaged in harm constitute legitimate targets in wartime, and action against legitimate targets must be proportionate to the threat they pose.[152]

These *jus in bello* principles are embodied, for example, in Article 52 of Additional Protocol I of the Geneva Conventions.[153] That Article provides that "civilian objects shall not be the object of attack or of reprisals."[154]

---

[147] Guilfoyle, Paige & McLaughlin, *supra* note 130, at 679.
[148] U.N. Charter art. 27, ¶ 3.
[149] *See* BRIAN OREND, THE MORALITY OF WAR 111–51 (2d ed. 2013).
[150] *Id.* at 11.
[151] *See id.* at 112–26.
[152] *See id.*
[153] Geneva Convention Relative to the Protection of Victims of International Armed Conflicts, art. 52, Aug. 12, 1949, 1125 U.N.T.S. 3.
[154] *Id.* art. 52.1.

"Civilian objects" are defined as "all objects which are not military objectives."[155] "Military objectives," according to Article 52, "are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[156]

Jus ad bellum and *jus in bello* principles in the international law of war operate together with the law of neutrality. The Hague Convention V of 1907 holds that the territory of neutral powers—that is, of states who are not belligerents in an armed conflict—is inviolable, that troops, munitions of war or supplies of belligerents cannot be moved across neutral territory, and that neutral powers must not allow such transit.[157] It further states neutrals have a duty to prevent belligerents from erecting wireless telegraphy stations "for the purpose of communicating with belligerent forces on land or sea" and from using any preexisting stations "for purely military purposes, and which has not been opened for the service of public messages."[158] However, a neutral power "is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[159] Convention XIII states that "[b]elligerents are bound to respect the sovereign rights of neutral Powers and to abstain, in neutral territory or neutral waters, from any act which would, if knowingly permitted by any Power, constitute a violation of neutrality."[160] Belligerents are prohibited from using neutral ports or waters, including for erecting communications apparatuses.[161]

Taken together, these principles seem to suggest that Internet infrastructure could comprise a legitimate target in wartime depending on where it is located and how it is used; that Internet infrastructure on neutral territory should not be targeted; that belligerents should not construct, and neutrals should not allow the construction of, new war-related Internet infrastructure on neutral territory; but that neutrals do not have a duty to

---

[155] *Id*.
[156] *Id.* art. 52.2.
[157] Hague Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, arts. 1–5, October 18, 1907, 36 Stat. 2310.
[158] *Id.* arts. 3, 5.
[159] *Id.* art. 8.
[160] Hague Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War, art. 1, October 18, 1907, 36 Stat. 2415.
[161] *Id.* art. 5.

prevent belligerents from using otherwise available Internet infrastructure located in neutral territory.

All of these issues are addressed in the Tallinn Manual 2.0.[162] Rule 54 of Tallinn 2.0 addresses undersea Internet cables by referring to existing international law applicable to submarine communication cables.[163] Comment 15 to Rule 54 states that, absent armed conflict, "the infliction of damage to cables by a State is prohibited as a matter of customary international law since doing so would run contrary to the object and purpose of the law governing submarine cables."[164] Comment 16 provides that states may investigate the circumstances of suspected incidents of cable cutting. Comment 17 states that tapping a cable in territorial or archipelagic waters violates the sovereignty of the coastal state because submarine vehicles, which must be used to facilitate such tapping, must transit such waters on the surface. According to the Tallinn experts, however, such tapping does not violate the sovereignty of a state that laid or operates the cable, if different from the coastal state.[165] Further, according to the Tallinn experts, tapping cables in waters outside a state's sovereignty, including on the high seas, does not violate any state's sovereignty.[166]

Specifically regarding LOAC, Rule 99 of Tallinn 2.0 states that "[c]yber infrastructure may only be made the object of attack if it qualifies as a military objective."[167] The Manual adopts the definition of "military objectives" found in Additional Protocol I.[168] The Comments provide examples of military objectives in cyberspace, including military command and control cyber systems, a SCADA system that controls the water flow from a reservoir above the location where troops are or may be stationed, a civilian air traffic control system used by the military when military systems have been damaged, and a website that passes coded messages to enemy forces.[169] Examples the Comments suggest would not qualify as military objectives could include "civilian data that is 'essential' to the well-being of the civilian population," a website that merely "inspir[es] patriotic sentiment

---

[162] Although the Tallinn Manual 2.0 is not part of any treaty or otherwise legally authoritative, it is widely recognized as a comprehensive restatement of international law principles applied to cybersecurity. *See generally* TALLINN MANUAL 2.0, *supra* note 120.
[163] *Id*. r. 54, at 252 (stating that "[t]he rules and principles of international law applicable to submarine cables apply to submarine communication cables").
[164] *Id.* r. 54, ¶ 15, at 256.
[165] *Id.* r. 54, ¶ 17, at 256.
[166] *Id.*
[167] *Id*. r. 99, at 434.
[168] *Id.* r. 100, ¶ 1 at 436.
[169] *See id.* r. 100, ¶¶ 8, 9, 15, 24, at 438, 440, 443.

among the population," any target that is "exclusively economic, political, or psychological," or the general Internet infrastructure upon which military networks might ultimately depend.[170] Further, according to the Comments, effects on civilian morale—for example by disrupting ordinary communications through a massive DNS attack—do not bear on whether the target is a legitimate military objective.[171]

Regarding the law of neutrality, the authors of Tallinn 2.0 note that neutrality principles focus on physical territory only because of 19th century context.[172] "The fact that cyberspace involves worldwide connectivity irrespective of geopolitical borders," they argue, challenges some of those baseline assumptions.[173] Tallinn 2.0's authors conclude that "[c]yber infrastructure located within the territory of a neutral State is not only subject to that State's jurisdiction, but also is protected by that State's territorial sovereignty," regardless of whether that infrastructure is publicly or privately owned.[174] The Manual defines "neutral cyber infrastructure" as "public or private cyber infrastructure that is located within the neutral territory (including civilian cyber infrastructure owned by a party to the conflict or nationals of that party) or that has the nationality of a neutral State (and is located outside belligerent territory)."[175] "Neutral territory" includes "the land territory of neutral States, as well as waters subject to their territorial sovereignty (internal waters, territorial sea, and, where applicable, archipelagic waters) and the airspace above those areas."[176]

Applying these principles, Rule 150 of the Manual prohibits attacks "by cyber means directed against neutral cyber infrastructure."[177] Rule 151 prohibits belligerents from launching cyber attacks into or across neutral territory, although a Comment notes that this would not prohibit "[u]sing a public, internationally and openly accessible network such as the Internet for military purposes" even if parts of the network are located in neutral territory.[178] Comments 1 and 2 to Rule 151 reference Article 5 of the Hague Convention V—which protects neutrals against military action by belligerents—in reference to the use by a belligerent of cyber infrastructure

---

[170] *Id.* r. 100, ¶¶ 7, 15, 20, 27–28, at 437, 440, 442, 444.
[171] *Id.* r. 100, ¶ 26, at 443.
[172] *See id.* ch. 20., ¶ 4, at 554.
[173] *Id.*
[174] *Id.* ch. 20., ¶ 5, at 554.
[175] *Id.* ch. 20 intro., ¶ 2, at 553.
[176] *Id.*
[177] *Id.* r. 150, ¶ 2, at 555.
[178] *Id.* r. 151, ¶ 4, at 556.

on neutral territory for military purposes.[179] The experts who deliberated over this provision were divided about whether such military use could include the transmission of cyber weapons (i.e., malware) on cyber infrastructure across neutral territory.[180] Tallinn 2.0 Rules 150 and 151 expressly refer only to the exercise of belligerent rights "by cyber means," perhaps intentionally leaving the issue of malware transmission unresolved"[181]

These definitions, Rules, and Comments in the Manual seem to suggest that portions of Internet cables lying on the seabed of the high seas are not "neutral" cyber infrastructure, regardless of who owns or controls the cables, as those portions fall outside the territory of a neutral state. Rather, they absorb the characteristics of the high seas themselves as territory not controlled by any state. If this is the correct reading, then the Tallinn 2.0 authors hold that the law of neutrality does not apply to portions of cables on the high seas. In that case, cables may be used to launch cyber attacks and also may themselves be attacked by physical or cyber means on the high seas so long as they are legitimate "military objectives," just like warships on the high seas.

Comment 2 to Rule 150 of the Manual, however, seems to take a different tack: "[n]eutral cyber infrastructure physically located in international airspace, *high seas areas*, or outer space is protected by virtue of the State of nationality's sovereignty."[182] It seems impossible to reconcile this Comment with the definitions of "neutral cyber infrastructure" and "neutral territory" that introduce the chapter on neutrality.

Consistent with what appears to be the implication of Tallinn 2.0, some state practice starting in the early 20th century seems to reflect the belief that undersea cables are proper military targets. Douglas Burnett, for example, cites as examples of state practice the 1914 destruction of a British telegraph cable station by a German Navy cruiser; the cutting of five German cables by the British cable ship *Alert* in 1914; the cutting of telegraph cables running out of New York by a German U-boat in 1918 and a similar effort by

---

[179] *Id.* r. 151, ¶¶ 1–2, at 556

[180] *Id.* r. 152, ¶ 3, at 558–59. Comment 6 to Rule 151 further suggests that the transmission of a "complete" cyber weapon in contrast to a packetized transmission would not tip the scales in either direction. In fact, the entire discussion of military use and malware transmission in Rules 151 and 152 seems curiously obtuse about how the Internet works. Internet protocols *always* break data into packets, and the sender generally cannot control the route any specific packet takes. These rules seem more suited to peer-to-peer networks or delivery through physical portable drives than to transmission of malware using the Internet.

[181] *Id.* r. 150–51, at 555–58.

[182] *Id.* r. 150, ¶ 2, at 555 (emphasis added).

a U-boat off Massachusetts also in 1918; and some other unspecified cable-cutting by Britain at the outset of both World Wars I and II.[183] These are important examples, but they date from an era when telegraph cables carried limited quantities and types of information and were not as central to the global economy as the present-day Internet. It is harder to claim that a core infrastructure component of a network that carries 52 trillion books' worth of information every day encompassing every field of human experience is a properly limited military target.

Burnett also cites the *Eastern Extension* case, which is a report of an arbitral award concerning the United States Navy's destruction of submarine cables owned by a private British company in Manila Bay during the Spanish-American War.[184] *Eastern Extension*, however, seems to stand for a much narrower proposition than Burnett suggests. At the time, the Philippines was a Spanish territory.[185] The *Eastern Extension* decision, issued in 1923 but relating to actions in 1898, noted that, because the British company operated under the authority of the Spanish Government, it could not be considered a neutral and the cables lacked "international character."[186] According to the tribunal:

> [I]t is almost unnecessary to recall that principle of international law which recognizes that the legitimate object of sea warfare is to deprive the enemy of those means of communication, which the high seas, in their character as *res nullius* or *res communis* afford to every nation. The use

---

[183] Douglas R. Burnett, *Submarine Cable Security and International Law*, 97 INT'L L. STUD. 1659, 1673–74 (2021).
[184] *Id.* at 1674.
[185] Events leading up to the Spanish-American war included challenges to Spanish authority in the Philippines by insurgents led by Emilio Aguinaldo, who was exiled in 1897 after a mediation ended the insurgency. After the decisive naval battle in Manila Bay, Aguinaldo returned from exile and led another insurgency, finally declaring the existence of the First Philippine Republic. Collusion between the Spaniards and Americans, however, enabled the United States to control the city of Manila. The United States refused to recognize the Philippine Republic, but instead annexed the Philippines under the Treaty of Paris that ended the Spanish-American War. This resulted in another insurgency and a further history of occupation and violence under U.S. custody and later, during World War II, under Japanese occupation. The United States did not relinquish its claim to sovereignty in the Philippines until 1946. *See generally* LOUIS A. PÉREZ, JR., THE WAR OF 1898: THE UNITED STATES AND CUBA IN HISTORY AND HISTORIOGRAPHY 1–23 (1998); BRIAN MCALLISTER LINN, THE PHILIPPINE WAR, 1899-1902 (2000).
[186] Eastern Extension, Australasia & China Tel. Co., Ltd. (Great Britain) v. United States, 6 R.I.A.A. 112, 113 (1923).

> by the enemy of that communication by sea, every belligerent, if he can, is entitled to prevent, subject to a due respect for innocent neutral trade; he is even entitled to prevent its use [sic] by neutrals, who use it to afford assistance to the enemy either by carrying contraband, by communicating with blockaded coasts, or by transporting hostile despatches, troops, enemy agents, and so on. . . . [I]t may be said that a belligerent's principal object in maritime warfare is to deprive the enemy of communication over the high seas while preserving it unimpeded for himself.[187]

Although this language seems to legitimize the destruction of undersea cables on neutral territory or on the high seas, in fact, the cables were cut on the seabed of the internal waters of a belligerent.[188] One landed in Capiz (another city in the Philippines) and the other landed in Hong Kong.[189] The Hong Kong cable was cut following a naval battle when the Spanish refused an American request for joint use of the cable to communicate with Hong Kong.[190] The cable cutting, then, occurred entirely within belligerent territory and cut off only the belligerent's ability to communicate by telegraph internally and with Hong Kong. These facts differ significantly from Internet cables on the seabed of the high seas carrying huge volumes of packets to and from locations all around the world.

Like Burnett, James Kraska argues that the Tallinn Manual's position in Rules 150 and 151 is mistaken and that the *Eastern Extension* case was correctly decided.[191] As Kraska notes, "Military information packets sent by a belligerent state are indistinguishable from ordinary Internet traffic and the specific pathways of information through submarine cables is unpredictable and uncontrollable."[192] Kraska therefore concludes that "the virtual cyberspace within submarine cables, like the airwaves, constitutes a global electromagnetic domain that is open to belligerents."[193]

---

[187] *Id.* at 115.
[188] *Id.* at 113.
[189] *Id.*
[190] *Id.* This request by the Americans seems strange, but it appears to reflect 19th century military etiquette norms, and, at the time, might have avoided fighting with land forces to secure the telegraph station.
[191] James Kraska, *The Law of Maritime Neutrality and Submarine Cables*, EJIL: TALK! (July 29, 2020), https://www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/ [https://perma.cc/X5WN-M7VE].
[192] *Id.*
[193] *Id.*

Kraska's observation about the indistinguishability of belligerent and neutral Internet packets is technologically correct, but his conclusions confuse three different considerations: (1) a neutral state's right or ability to exclude belligerents from sending ordinary communications packets over neutral Internet cables; (2) a belligerent's ability to launch cyberattacks—i.e., to send malicious packets—that may travel over undersea Internet cables controlled by a neutral or within neutral territory; and (3) the duty of belligerents to avoid damage to the physical cables controlled by a neutral or under a neutral's jurisdiction.

Most of Kraska's argument seems directed to consideration (1). Here, his reference to "the virtual cyberspace *within* submarine cables" and analogy to the airwaves makes some sense.[194] The question is whether the neutral state can take action to cut off communications of a belligerent in the form of electromagnetic radiation that traverses the neutral's territory. Certainly, the neutral cannot damage or destroy physical transmission equipment, such as antennas, located in the belligerent's territory, without thereby forfeiting its status as a neutral. But the neutral could utilize jamming equipment physically located within its own territory to impede the belligerent's signals as they travel over the airwaves without surrendering neutrality. Just as a State has the right to control its territorial waters, it has the right to control its territorial skies and airwaves, without sacrificing neutrality.[195]

Likewise, a neutral undoubtedly has the right to control physical Internet infrastructure located within its territory, including undersea cables within territorial waters, landing stations that receive undersea cables, terrestrial IXPs, and all the other multifarious components of the Internet's physical layer on land. Censorship of Internet traffic relating to certain subjects or flowing into or out of certain territories involves international human rights concerns, but it does not turn the censoring nation into a belligerent in armed conflict.[196]

---

[194] *Id.* (emphasis added).

[195] *See, e.g.*, Convention on International Civil Aviation, art. 1, Dec. 7, 1944, 15 U.N.T.S. 295 (affirming that "every State has complete and exclusive sovereignty over the airspace above its territory"); International Radiotelegraph Convention, art. 3, § 1, Nov. 25, 1927, T.S. No. 767 (noting the liberty of each State to determine types of communications services and classes of communications).

[196] For a discussion of such censorship, how it happens technologically, and some of the human rights concerns involved, see, e.g., Allie Funk, Kian Vesteinsson & Grant Baker, *Freedom on the Net 2024*, FREEDOM HOUSE (2024), https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online

The second consideration about belligerents sending packets related to malware over neutral cyber infrastructure requires more nuance. There is no doubt that a neutral, consistent with its domestic criminal, national security, cybersecurity, and privacy laws, could utilize measures designed to *disrupt* the transmission of malware, the functioning of botnets, and so-on, without thereby becoming a participant in any armed conflict. But whether a belligerent violates neutrality by *sending* packets relating to malware that traverse a neutral's cyber infrastructure presents a more difficult question. The issue is one of practicality and of other policy concerns—what is actually possible and desirable if the global Internet is to retain its relatively free and decentralized character—rather than of LOAC.

If the rule is that neutrality is violated whenever any malware packet sent by a belligerent crosses a neutral's cyber infrastructure, then any delivery of malware as a weapon of war over the Internet would effectively be barred. It is simply impossible to rule out that a packet might cross neutral cyber infrastructure. As Kraska notes, "[i]mplementation of the Tallinn Manual 2.0 rules appears to presume a level of control required by belligerents to avoid cables lying in neutral waters or neutral cables on the deep seabed that almost certainly is unrealistic."[197] This may or may not be a good policy result from the perspective of constraining armed conflict, but it does not seem to be what Tallinn 2.0 intends.

At the same time, these practical difficulties, in the decentralized Internet context, cannot simply authorize belligerents to commandeer, damage, or destroy cyber infrastructure anywhere in the world at any time. Such an extreme result does not seem to be Burnett or Kraska's intent. In fact, Kraska's broad use of the term "undersea" suggests that *Eastern Extension* is not really on point at all, since that case involved landing stations and cables within territorial waters. The question returns to the possible ambiguity in Tallinn 2.0 about whether neutrality in fact applies to portions of cables *outside* internal, territorial, and archipelagic waters, that is, portions lying on the seabed of the high seas.

Here, Kraska attempts to separate the content and physical layers with an analogy to transmission over the airwaves. According to Kraska,

---

[https://perma.cc/5R5J-3W9L]. Of course, not all "censorship" is bad from a human rights perspective: it is good to censor malware attacks, CSAM, and the like.

[197] Kraska, *supra* note 191.

> The law of neutrality was developed based on actions in the physical domain—the sanctity of neutral waters, for example. Submarine cables, while consisting of a physical infrastructure, serve as a medium of transmission and operate much like the airspace, within which radio waves propagate at will. Travel by ship through neutral waters implicates the law of neutrality, so too does flight in national airspace. But broadcasting radio waves through neutral national airspace does not by itself affect state sovereignty in the same way, since it is not a tangible physical activity.[198]

This analogy does not hold. Transmissions over the airwaves, by definition, do not occur within any human-made container. In contrast, whatever happens within a submarine Internet cable occurs entirely within the discrete, identifiable physical space of the human-made cable.[199] In the context of submarine cables, the Internet's physical backbone is very tangibly physical. Cables are not analogous to airspace, nor to the seas themselves; they are specific things *in* the seas and *on* the seabed. While it might not be practical to preclude certain packets from traveling on cables owned or controlled by neutrals, whether on the high seas or otherwise, it is perfectly reasonable to identify specific cables lying on the seabed of the high seas as extensions of neutral territory that cannot be physically tampered with. This is no different than recognizing that ships sailing on the high seas are within the sovereignty of their flag.

Tallinn 2.0, then, for the most part soundly applies basic principles of the law of the sea and principles of LOAC to cyber infrastructure. Nevertheless, it contains ambiguities and even contradictions concerning whether cables owned or controlled by neutrals lying on the seabed of the high seas are protected by the law of neutrality. Moreover, the standard for what comprises a military objective, whether an undersea Internet cable is owned or controlled by belligerents or neutrals, is quite broad. There is little doubt that Internet communications infrastructure makes an "effective

---

[198] *Id*.

[199] Of course, Internet cables, like any cable that carries electromagnetic signals, might produce some electromagnetic field leakage, although in fiberoptic cables this will be minimal. Undersea cables also might be engineered to produce an RF signal so that they can be located for maintenance purposes. But all of the data transmission occurs entirely within the cable.

contribution to military action" and that its "total or partial destruction, capture or neutralization" would offer a definite military advantage.[200]

Finally, even if LOAC offered a clear standard for protecting Internet cables lying on the seabed of the high seas, its practical effect would be limited without commitments from the world's naval powers to enforce neutrality. Current U.S. Naval doctrine emphasizes the general importance of deterrence:

> The presence of naval forces or their movement to a crisis area are two of the strongest deterrent signals we can send. They are unequivocal evidence that a fully combat-ready force stands poised to protect our national interests, and that additional force whatever it takes will be forthcoming. Our naval forces are the leading edge of the world's most capable military, and their well-understood ability to project power is a key factor in deterrence. Forward deployed naval forces are available to respond quickly, require minimal support, and are not restricted in their movements. They are available for diplomatic, political, and economic deterrent actions that can influence, persuade or pressure uncooperative governments around the world to choose peaceful means of achieving their goals.[201]

U.S. naval doctrine further states that:

> [o]ur nation routinely calls upon naval forces independently or as part of joint task forces to exercise two fundamental elements of our national military strategy: forward presence and crisis response. . . . [N]aval forces may be tasked to conduct such contingency activities as shows of force, freedom-of-navigation operations, combat operations associated with short duration interventions, and post-combat restoration of security.[202]

Forward presence and crisis response operations can include enforcing U.N. sanctions, combatting terrorism, and assisting other nations in

---

[200] TALLINN MANUAL 2.0, *supra* note 120, r. 100, at 435.
[201] NAVAL DOCTRINE PUBLICATION 1: NAVAL WARFARE 17–18 (1994) https://www.govinfo.gov/content/pkg/GOVPUB-D207_400-PURL-LPS2123/pdf/GOVPUB-D207_400-PURL-LPS2123.pdf [https://perma.cc/7PPH-USU9].
[202] *Id.* at 21.

self-defense, among other things.[203] Further, U.S. naval doctrine asserts that control of the sea allows the Navy to "protect sea lines of communication."[204]

There is little doubt, then, that the United States or a naval coalition including U.S. forces, perhaps acting under U.N. auspices, could conduct patrols focused on the integrity of undersea Internet infrastructure. Nothing in the Biden or Trump administrations' cyber or military policies, however, suggests any specific thought about how the U.S. Navy might protect subsea Internet cables owned by U.S. companies or by neutrals against violations of LOAC by other countries or their proxies. This appears to be an issue of resources and priorities. The reality is that undersea Internet infrastructure is distributed across vast areas of the world's oceans and becomes an afterthought until a specific conflict arises. It cannot effectively be protected primarily by LOAC and military power

III. INTERNET GOVERNANCE, MARKETS, AND LOCAL REGULATION

Part II summarized possible international law responses to undersea Internet cable-cutting. While these options are all of limited utility for specific reasons, there is an overarching theme: the post-Westphalian norms and rules of international law were not designed for the global Internet age. Hugo Grotius never imagined the scale and speed of a communications and cultural system like the Internet. The vulnerability of undersea Internet cables raises questions of Internet governance and the uniqueness or lack of uniqueness of cyberspace.[205] This Part reviews market and private and public law options that have grown up alongside the Internet, including redundancy and repair capacity, market concentration and antitrust, and licensing requirements for cable landing stations. It suggests that these solutions, based in markets, contracts, and discrete interventions for market failures, are necessary adjuncts to possible changes in the Law of the Sea or LOAC.

---

[203] *Id.* at 22.
[204] *Id.* at 26.
[205] For additional background on notions of Internet exceptionalism, *see* David W. Opderbeck, *Cybersecurity and Executive Power*, *supra* note 27, at 829–36; David W. Opderbeck, *Copyright in AI Training Data: A Human-Centered Approach*, *supra* note 27, at 1004–06.

A. Redundancy and Private Repair Capacity

Although commentators recognize the role of private companies and consortia in laying and operating undersea Internet cables, as suggested in the summary of proposals in Part II, most proposed remedies for cable sabotage focus on international law of the sea and LOAC principles that govern States. The international law scholars who have considered the question still mostly conceptualize undersea cables as discrete pieces of hardware rather than as components of the global Internet. In other words, they have not seen that this is an *Internet governance* problem and not just a *law of the sea* problem.[206]

This makes the problem even more challenging because international law, including the law of the sea, is rooted in Westphalian ideas of state sovereignty, while the Internet's core underlies a transnational network.[207] The international community has taken steps in recent years towards norms for global governance of the Internet's core. This includes work by the Netherlands Scientific Council for Government Policy led by Dennis Broeders, the Paris Call for Trust and Security in Cyberspace, and reports by the 2019–2021 UN Group of Governmental Experts (UN GGE) and the 2019–2021 UN Open-Ended Working Group (OEWG) on cyber security.[208] These developing norms are relatively weak because they are voluntary and non-binding.[209] Their voluntary character reflects the transnational, bottom-up architecture and technical governance structure of the global Internet.

Ironically, then, the continued *privatization* of the undersea Internet hardware layer might prove its most realistic defense against sabotage. As the OEWG Report recognized, Internet "infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States" and, "[a]s a result, inter-State or

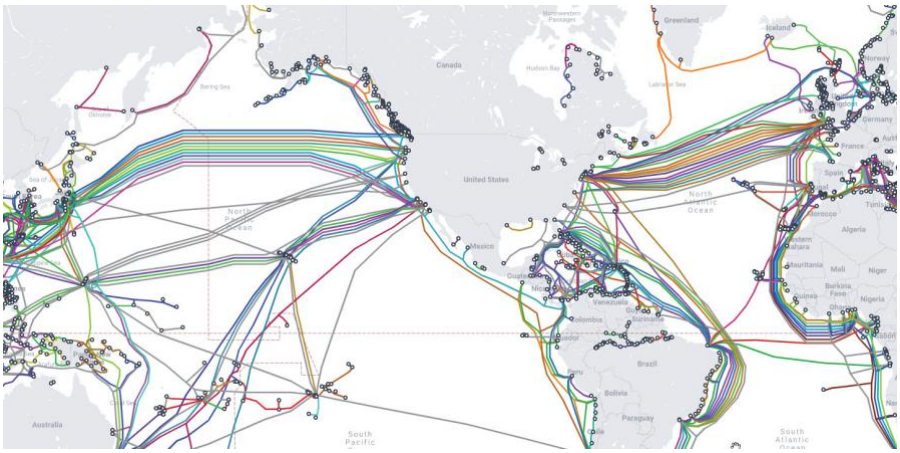
---

[206] *Cf.* Dennis Broeders & Arun Sukumar, *Core Concerns: The Need for a Governance Framework to Protect Global Internet Infrastructure*, 16 POL'Y & INTERNET 411 (2024).
[207] *See id.* at 418–21. As Broeders and Sukmar note, "[p]ublic core infrastructure exists to support global Internet governance, which cannot be the *domaine réservé* of any single state." *Id.* at 419.
[208] DENNIS BROEDERS, THE PUBLIC CORE OF THE INTERNET: AN INTERNATIONAL AGENDA FOR INTERNET GOVERNANCE (2015); *Cybersecurity: Paris Call for Trust and Security in Cyberspace*, PERMANENT MISSION OF FRANCE TO THE U.N. (Nov. 12, 2018), https://onu.delegfrance.org/Cybersecurity-Paris-Call-for-Trust-and-Security-in-Cyberspace [https://perma.cc/V9L3-3TUE] (last visited Apr. 6, 2026); U.N. GOAR *Final Substantive Report*, U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021) [hereinafter OEWG REPORT]; U.N. GAOR, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, U.N. Doc. A/76/135 (July 14, 2021) [hereinafter 2021 GGE REPORT]; Broeders & Sukmar, *supra* note 206, at 416–17.
[209] *See* 2021 GGE REPORT, *supra* note 208, ¶ 15; OEWG REPORT, *supra* note 208, ¶ 24.

public-private cooperation may be necessary to protect its integrity, functioning and availability."[210]

This dynamic reflects the bottom-up ethos of the Internet's design. Packet-switched networks, the Internet's foundational technology, were first developed, in part, in pursuit of communications networks that could withstand the disruptions of war, including nuclear war.[211] Since the internet working protocols allowed packets to travel along the most efficient route, a disruption along one pathway would not prove fatal—*if* the overall internet working structure included multiple nodes and pathways over which packets could travel between the origination and destination points. The more nodes and pathways incorporated into the network, the less likely any localized disruption would cause a communication failure.

At present, undersea Internet cables are vulnerable because there are not enough of them. Telegeography's often cited submarine Internet cable map looks impressive, but it shows only about 600 cables worldwide.[212]



[210] OEWG REPORT, *supra* note 208, ¶ 18.
[211] Christopher Yoo, *Paul Baran, Network Theory, and the Past, Present, and Future of the Internet*, 17 COLO. TECH. L. J. 161, 164 (2018).
[212] *See Submarine Cable Map*, TELEGEOGRAPHY, https://www.submarinecablemap.com/ (last visited Apr. 19, 2026). The colors indicate cable ownership. For information about how the map is constructed, *see Submarine Cable Frequently Asked Questions*, TELEGEOGRAPHY, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions [https://perma.cc/9SKR-8TF4] (last visted Apr. 6, 2026).

There are only 17 cables between Europe and North America.[213] These cables appear densely concentrated on the map, but the northernmost and southernmost cables lie hundreds of nautical miles apart. An operation to cause significant damage to this group of cables in a short period of time would necessarily involve multiple ships operating at once along a broad swathe of the Atlantic Ocean. The same could be said for cables leaving the west coast of the United States and crossing the Pacific. Of course, some more remote locations are served by fewer connections, and are far more vulnerable—for example, Greenland, with one cable, or Iceland, with four.

In either case—whether a region already has relatively robust undersea connectivity or not—as a practical matter, the best defense against cable sabotage is more connectivity and more repair capacity.[214] If there are more potential routes for packets to travel under the seas—or over the skies, via satellite—the sabotage game will not be worth the candle. The question is whether the private market will supply these additional routes and whether this result is healthy for Internet governance.[215]

Repair capacity is an often-overlooked factor. The undersea cable industry suggests that "[c]able faults are really common."[216] According to industry data, about four cable faults occur each week, with two-thirds of all faults attributed to "external aggression."[217] This data point seems alarming, but the industry uses "external aggression" as a term of art that includes inadvertent damage by fishing and transport vessels.[218]

The industry suggests that the most effective regulatory interventions would include limitations on fishing near cable routes, publishing cable route information, requiring fishing vessels to employ automated identification

---

[213] Alan Mauldin, *Cutting Off Europe? A Look at How the Continent Connects to the World*, TELEGEOGRAPHY (Oct. 13, 2022), https://blog.telegeography.com/cutting-off-europe-a-look-at-how-the-continent-connects-to-the-world#:~:text=Europe%20is%20connected%20to%20North,a%20few%20other%20intercontinental%20options [https://perma.cc/67J3-29ZZ].

[214] *See* Lane Burdette, *What to Know About Submarine Cable Breaks*, TELEGEOGRAPHY (Nov. 21, 2024), https://blog.telegeography.com/what-to-know-about-submarine-cable-breaks [https://perma.cc/A6KY-4FY4] (stating that "[b]y spreading their networks' capacity over multiple cables, operators ensure that if one breaks, their network will run smoothly over the others until the damage is repaired").

[215] *See infra*, Part III.B.

[216] Tim Stronge, *Is it Sabotage? Unraveling the Mystery of Undersea Cable Breaks*, TELEGEOGRAPHY (Feb. 3, 2025), https://blog.telegeography.com/is-it-sabotage-unraveling-the-mystery-of-undersea-cable-breaks [https://perma.cc/64B2-K5EX].

[217] *Id.*

[218] *Id.*; *see also* Burdette, *supra* note 214.

systems (AIS) and vessel monitoring systems (VMS), limiting the deployment of fish aggregating devices (FADs), creating lifecycle registries of FADs, limiting deep sea mining near cable routes, expanding cable protection zones, and reducing regulatory and customs barriers to the operation of cable-laying and repair ships.[219] Industry leaders acknowledge that some recent incidents in the Baltic seem suspicious but wish to divert attention away from intentional state action.[220] In other words, the industry wants a favorable regulatory environment, sees its main competitor for regulatory space as the commercial fishing industry, and is worried that a focus on international conflict might impact its freedom to operate.

B. Market Concentration as a Governance Problem

Some of the industry's proposals might have merit, but they are also self-serving and ignore potential problems from market concentration. Within the three Tiers of Internet infrastructure, there are many providers of last mile Tier 3 and 2 services, but Tier 1 markets are more concentrated.[221] There are only about 14 Tier 1 Internet backbone providers globally. Even before Google, Amazon, Microsoft, and Meta entered the undersea cable business, the consortia that controlled existing cables potentially wielded significant market power. At the hardware layer, then, Internet governance lies in the hands of a very small number of powerful private companies. In merely economic terms, this raises the possibility of market failures. In governance terms, it produces a democratic and rule-of-law deficit.

About 98% of undersea cables are manufactured and installed by only four firms—SubCom in the United States, Alcatel in France, Nippon Electric

---

[219] INT'L CABLE PROT. COMM., GOVERNMENT BEST PRACTICES FOR CABLE PROTECTION AND RESILIENCE, VERSION 1.2, 2–3 https://www.iscpc.org/documents/?id=3733 [https://perma.cc/25KL-FJCD] (last visited Feb. 24, 2026). According to its website, the ICPC "was founded in 1958 and its Membership comprises of governmental administrations and commercial companies that own or operate submarine telecommunications or power cables, as well as other companies that have an interest in the submarine cable industry—including most of the world's major cable system owners and cable ship operators." *About the ICPC*, INT'L CABLE PROT. COMM. (Jan. 14, 2026), https://www.iscpc.org/about-the-icpc/ [https://perma.cc/8VXL-QLYC].

[220] *See* Stronge, *supra* note 216 (asking "[s]o, what's behind the most recent cable faults? I don't really know," but concluding that "[i]f the intent of sabotage is to send a signal, you could argue that such a campaign has failed. Severing a few cables in an industry habitually accustomed to repairing 200 faults each year is not a signal . . . it's just noise.").

[221] *See ISP Tiers*, CISCO: THOUSANDEYES , https://www.thousandeyes.com/learning/techtorials/isp-tiers [https://perma.cc/VL9Z-JEUY] (last visited Feb. 24, 2026).

in Japan, and HMN Technologies in China.[222] Most are owned by individual companies or consortia of companies involving Tier 1 providers.[223] The hyperscalers Amazon, Google, Meta, and Microsoft are increasingly driving growth, and they now control cables that carry about half the total available subsea bandwidth.[224]

This potential market concentration problem spurred legal battles over "network neutrality" that have raged since the early 2000s. The focus of the network neutrality debate was on whether backbone providers—that is, Tier 1 or 2 networks—should be prohibited from prioritizing or slowing down packets based on their source. Providers argued that prioritization decisions should be left to the market.[225] If, for example, a provider reached a commercial deal to prioritize packets from Netflix and not Hulu, another provider might instead reach a deal to prioritize Hulu, while yet another provider might not prioritize either, and the market would sort out which models consumers preferred. Network neutrality advocates argued that market concentration for backbone services would preclude robust, flexible competition, to the detriment of newer edge services and of edge services with more niche or controversial content.[226]

---

[222] Erin L. Murphy & Matt Pearl, *China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts*, CTR. FOR STRATEGIC AND INT'L STUDS. (Apr. 4, 2024), https://www.csis.org/analysis/chinas-underwater-power-play-prcs-new-subsea-cable-cutting-ship-spooks-international [https://perma.cc/9MAY-KMKS].

[223] *Id.*

[224] *Id.*; *see generally* Peter Gervasi, *Diving Deep Into Submarine Cables: The Undersea Lifelines of Internet Connectivity*, KENTIK (Mar. 28, 2023), https://www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity/ [https://perma.cc/24FK-9563]; Alan Mauldin, *A (Refreshed) List of Content Providers' Submarine Cable Holdings*, TELEGEOGRAPHY (June 27, 2024), https://blog.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list-new [https://perma.cc/NDX7-HK7A]; Joe Brock, *U.S. and China Wage War Beneath the Waves—Over Internet Cables*, REUTERS (Mar. 24, 2023), https://www.reuters.com/investigates/special-report/us-china-tech-cables/ [https://perma.cc/AT5K-TFBV].

[225] *See, e.g.*, Jon Miltimore, *Net Neutrality is Not About 'Saving the Internet.' It's About Controlling the Internet*, FOUND. FOR ECON. EDUC. (May 30, 2024), https://fee.org/articles/net-neutrality-is-not-about-saving-the-internet-its-about-controlling-the-internet [https://perma.cc/MVY3-K7TS].

[226] *See, e.g.*, *Net Neutrality*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/net-neutrality [https://perma.cc/GY32-2DJS]; *Sixth Circuit Rules Against Net Neutrality; EFF Will Continue to Fight*, ELEC. FRONTIER FOUND. (Jan. 7, 2025), https://www.eff.org/deeplinks/2025/01/sixth-circuit-rules-against-net-neutrality-eff-will-continue-fight [https://perma.cc/EH5W-DM6R].

The most recent set of network neutrality rules, *Safeguarding and Securing the Open Internet*; *Restoring Internet Freedom* (the "Safeguarding Order" or the "Order"), adopted by the FCC towards the end of the Biden Administration in 2024, were set aside by the Sixth Circuit in January 2025 as an improper interpretation of the Telecommunications Act of 1996.[227] The Safeguarding Order noted threats to cybersecurity including Chinese espionage through compromised telecommunications firms, logic bombs in U.S. critical infrastructure, and persistent access to computing infrastructure, and argued that the reclassification of broadband Internet service "significantly bolster[s] the Commission's existing authority to take regulatory actions to address cybersecurity risks and vulnerabilities in broadband networks."[228] It did not, however, mention threats to undersea cables, nor did it include any rules relating to cybersecurity.

The Safeguarding Order also mentioned the resilience and reliability of broadband communications networks particularly during natural disasters and other emergencies.[229] According to the Safeguarding Order, reclassification would "secure the Commission's authority to, as necessary,

---

[227] *Safeguarding and Securing the Open Internet; Restoring Internet Freedom*, 89 Fed. Reg. 45404 (May 22, 2024) [hereinafter Safeguarding Order]; In re MCP No. 185, 124 F.4th 993 (6th Cir. 2025). The Sixth Circuit heard consolidated appeals referred by the Judicial Panel on Multidistrict Litigation. *Id.* at 1000–01. The basic issue is whether the FCC can classify broadband Internet as a "telecommunications service," which would trigger common carrier regulations encompassing network neutrality, or whether broadband Internet must be classified as an "information service," which would entail a lighter regulatory touch. *Id.* at 999–1000. In 2005, the Supreme Court held that under the *Chevron* doctrine the FCC had authority to classify cable modem services as an "information service." Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005). In 2015, the FCC under the Obama Administration classified broadband Internet as a "telecommunications service" subject to common carrier rules and issued network neutrality rules. *Protecting and Promoting the Open Internet*, 80 Fed. Reg. 19737 (Apr. 13, 2015). The FCC's authority to make this classification and issue these rules was also upheld by the D.C. Circuit under the *Chevron* doctrine. U.S. Telecomm. Ass'n v. FCC, 825 F.3d 674 (D.C. Cir. 2016), *reh'g en banc denied*, 855 F.3d 381 (D.C. Cir. 2017), *cert. denied*, 586 U.S. 994 (2018). When the FCC reversed course under the first Trump administration, the D.C. Circuit further upheld the FCC's authority under the *Chevron* doctrine to reclassify broadband Internet, once again, as an information service. Mozilla Corp. v. FCC, 940 F.3d 1 (D.C. Cir. 2019) (per curiam). By the time the Biden Administration's *Safeguarding Order* reached the Sixth Circuit, however, the Supreme Court had overruled the *Chevron* doctrine. *See* Loper Bright Enters. v. Raimondo, 603 U.S. 369 (2024). The Sixth Circuit's subsequent *In re MCP No. 185* decision held that *Brand X* and the previous D.C. Circuit decisions on network neutrality rules were no longer good law, although the court ultimately held that the FCC's Order was barred by the plain meaning of the statute.

[228] Safeguarding Order, 89 Fed. Reg. at 45406.

[229] *Id.* at 45406–11.

implement requirements for network upgrades and changes, adopt rules relating to recovery from network outages, and improve our incident investigation and enforcement authority to mitigate network threats and vulnerabilities."[230] Again, however, the Order did not specifically mention undersea cables or include any rules relating to physical security or resilience.

While giving lip service to cybersecurity, the Safeguarding Order noted that the FCC would exercise forbearance in the application of interconnection rules for telecommunications services.[231] Sections 251–252 within Title II of the Telecommunications Act of 1996 set forth duties of interconnection and related obligations of telecommunications providers under which the FCC has enacted detailed rules applicable to telephone carriers.[232] The Commission noted that the general interconnection requirements for common carriers in sections 201–202 of the 1934 Act and the incentives for broadband penetration in section 706 were sufficient to address interconnection issues relating to broadband Internet service.[233] In other words, the FCC recognized the policy judgment in the 1996 Act that broadband Internet should receive a light regulatory touch. As a result, even when network neutrality rules have been in effect, the FCC has never adopted interconnection rules for broadband internet.

The Safeguarding Order would, however, have imposed the requirements in section 214 of the Communications Act to broadband providers.[234] Section 214 requires any "carrier" to obtain a certificate of convenience and necessity from the FCC before constructing any new "line," extending any existing line, or acquiring or operating a line or extension.[235] The FCC must notify the Secretary of State and the Secretary of Defense of any such application and those Departments have a "right. . . to be heard."[236] Starting in 1999, the FCC issued blanket approval for new construction by

---

[230] *Id.* at 45413.
[231] *Id.* at 45486–90.
[232] *Id.* at 45486–87.
[233] *Id.* at 45487; 47 U.S.C. §§ 201–202; 47 U.S.C. § 1302. Section 706 states that the Commission will encourage the deployment of broadband infrastructure through "price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment." 47 U.S.C. § 1302.
[234] Safeguarding Order, at 45406–07.
[235] 47 U.S.C. § 214.
[236] *Id*.

telecommunications carriers subject to the FCC's authority to *revoke* the blanket approval in specific cases.[237]

The Safeguarding Order referenced "cases where the Commission identified [national security] threats and revoked the authority of certain foreign-owned adversarial service providers to provide Title II telecommunications services (including 'traditional telephony') in the United States pursuant to its section 214 authority, but was not able to stop them from providing BIAS or other internet-based services that were then classified as Title I services."[238] According to the FCC, "[c]lassifying BIAS under Title II alleviates those concerns, restoring a broader range of regulatory tools and enhancing the Commission's jurisdiction to cover broadband services, providers, and networks."[239] The FCC also found that "reclassification will enable the Commission to make more significant national security contributions as we continue our longstanding coordination with our Federal partners."[240]

In recent years the FCC has invoked its Section 214 authority to revoke traditional telecom line approvals for Chinese Firms for national security reasons.[241] In *China (Unicom) v. FCC*, applying *Loper Bright,* the Ninth Circuit upheld the FCC's power to revoke licenses for these reasons under Section 214.[242] In a stinging dissent, Judge Bea complained that "The Lord giveth and the Lord taketh away. . . . Today, the majority declares that the Federal Communications Commission ("FCC") may act as the Lord in cancelling telecommunications certificates."[243]

C. Cable Landing Licenses and Cybersecurity

After the Sixth Circuit's ruling on the Safeguarding Order, of course, it is clear that—barring an unlikely Supreme Court reversal—the FCC cannot regulate broadband Internet under the common carrier rubric and therefore

---

[237] Implementation of Section 402(b)(2)(A) of the Telecommunications Act of 1996; Petition for Forbearance of the Independent Telephone & Telecommunications Alliance, Report and Order and Second Memorandum Opinion and Order, 14 FCC Rcd. 11364, 11365–66 (1999).
[238] Safeguarding Order, *supra* note 227, at 45405.
[239] *Id*.
[240] *Id*.
[241] *See* China Unicom (Ams.) Operations Ltd. v. FCC, 124 F.4th 1128 (9th Cir. 2024); China Telecom (Ams.) Corp. v. FCC, 57 F.4th 256 (D.C. Cir. 2022); Pac. Net. Corp. v. FCC, 77 F.4th 1160 (D.C. Cir. 2023).
[242] *China Unicom*, 124 F.4th at 1128.
[243] *Id.* at 1156–57 (Bea, J., dissenting).

cannot apply the Section 214 line approval rules or the Section 250–251 interconnection rules to broadband Internet services. The FCC does, however, possess explicit statutory authority to regulate licenses for submarine cable landings, including Internet cables, on U.S. soil pursuant to the Submarine Cable License Landing Act of 1921 and an Executive Order issued by President Eisenhower in 1954.[244]

The 1921 Cable Landing License Act originally required direct Presidential approval for cable landing licenses and the 1954 Executive Order delegated that authority to the FCC while also requiring approval by the Secretary of State.[245] The current FCC rule implementing this statute focuses on foreign ownership disclosures and related items, but does not include any specific cybersecurity obligations. However, the rule states "that licensee shall at all times comply with any requirements of United States government authorities regarding the location and concealment of the cable facilities, buildings, and apparatus for the purpose of protecting and safeguarding the cables from injury or destruction by enemies of the United States of America."[246] FCC practice since the early 2000s has been to refer cable landing license applications involving entities having foreign ownership or 10% or greater foreign direct investment to other executive branch agencies for additional review.[247] This includes review by an interagency group from the Departments of Defense, Homeland Security, and Justice known as "Team Telecom."[248]

Comprehensive Amendments to the FCC cable landing license rule relating to national security have been proposed five times since 2012, resulting in a Final Rule finally published on October 27, 2025.[249] In 2020, President Trump issued an Executive Order that meant to clarify the process for Team Telecom to review landing license applications for national security

---

[244] *See Submarine Cable Landing Licenses*, FCC, https://www.fcc.gov/research-reports/guides/submarine-cable-landing-licenses [https://perma.cc/V2T7-RUE6]; 47 U.S.C. § 34 (1921); Exec. Order No. 10530, 19 Fed. Reg. 2709 (May 12, 1954).
[245] Exec. Order No. 10530, *supra* note 244.
[246] 47 C.F.R. § 1.767(g)(3) (2025).
[247] *See Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, 35 FCC Rcd. 10927, 10928–30 (¶¶ 3–5) (2020).
[248] *Id.* at 10929–30 ¶5.
[249] *See* 77 Fed. Reg. 70,400 (Nov. 26, 2012); 80 Fed. Reg. 67689 (Nov. 3, 2015); 81 Fed. Reg. 46870 (July 19, 2016); 85 Fed. Reg. 65566–01 (Oct. 15, 2020); 88 Fed. Reg. 50486 (Aug. 1, 2023); *Review of Submarine Cable Landing License Rules and Procedures*, 90 Fed. Reg. 48648 (Oct. 27, 2025) [hereinafter Final Rule].

implications.[250] The FCC followed with an Order establishing specific processes and timelines for this review.[251] These procedures are focused entirely on foreign influence and do not address day-to-day cybersecurity procedures or any questions relating to the physical security of cables.[252] They were intended to streamline the application process while protecting the United States against undue foreign influence, but as one commentator has noted, they have resulted in "an unpredictable ordeal for applicants."[253]

On March 13, 2025, the FCC issued a Notice of Proposed Rule Making once again suggesting changes to the landing license rule.[254] A significant portion of the NPRM focuses on cybersecurity and physical resilience.[255] The NPRM noted that:

> [g]iven the role of submarine cables to the Nation's communications networks and other vital infrastructure and assets, it is important to ensure the protection, security, and resilience of this critical infrastructure. Accordingly, damage to submarine cable infrastructure would affect other critical infrastructure sectors that rely on communications and would have a debilitating impact on the Nation's economic and national security.[256]

The NRPM suggested a cybersecurity reporting and certification requirement aligned with the NIST Cybersecurity Framework and sought comment on safeguards over physical access, the relationship between logical, physical and remote access, and protections against physical damage and malicious physical threats.[257] It also requested comment on enhanced requirements for GIS location information about undersea cables including

---

[250] Exec. Order No. 13,913, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643 (Apr. 8, 2020). *See* RICHARD SALGADO, HOOVER INST., UNDERSEA CABLES, HYPERSCALERS, AND NATIONAL SECURITY 7–8 (2023), https://www.hoover.org/sites/default/files/research/docs/Salgado_finalfile_WebReadyPDF.pdf [https://perma.cc/KVC4-FTGX].
[251] Process Reform, *supra* note 247, at 10927–28 (¶¶ 3–5).
[252] *Id*.
[253] SALGADO, *supra* note 250, at 9.
[254] *Review of Submarine Cable Landing License Rules and Procedures*, 90 Fed. Reg. 12036 (Mar. 13, 2025).
[255] *Id.* at 12056–64 (¶¶ 85–119).
[256] *Id.* at 12062 (¶ 115).
[257] *Id.* at 12060 (¶¶ 104–06), 12062 (¶¶ 115–16).

the wet and landing portions.[258] The NPRM noted that the industry has previously expressed confidentiality concerns about such specific data and proposed intra-agency cybersecurity sharing procedures that the FCC believed would protect confidentiality.[259] The requirement for license applications to adopt cybersecurity and physical security risk management plans was incorporated in the Final Rule.[260]

Regulation along these lines is a positive development that was long overdue. However, some other elements of the FCC NPRM that were adopted in the Final Rule reflect troubling currents that could increase the trend towards nationalized "splinternets." The NPRM suggested lowering due process hearing requirements so that the FCC—and ultimately the President—could more easily refuse to issue a new license, or revoke an existing license, based on national security concerns.[261] This included a presumption or categorical qualifying condition against applicants owned, controlled, or "subject to the influence of" a foreign adversary country or an individual or entity on the Commission's Covered List.[262] A key stated concern here was foreign ownership of cable systems, landing stations, and other interconnections and the ability of law enforcement to serve process and gain access to cables for surveillance purposes.[263] The NPRM also connected cybersecurity requirements with the FCC "Covered List" of equipment manufacturers maintained under the Secure and Trusted Communications Networks Act of 2019, which currently includes the Chinese companies Huawei, ZTE, Hikvision, Dahua, and Hytera and invites comment on a possible rip and replace requirement for such equipment.[264]

The Final Rule adopted these proposals with some modifications responding to concerns raised by the industry in submitted comments relating to the breadth of the phrase "subject to the influence of."[265] None of the commenters objected to the presumptive disqualifying condition, which was incorporated into the Final Order.[266] The Final Order also adopted a disqualifying presumption relating to "character qualifications," which relates not only to past violations of the Cable License Landing Act and related rules, but also to any applicant who "[m]ade materially false statements or

---

[258] *Id.* at 12054–56 (¶¶ 77–82).
[259] *See id.* at 12056 (¶ 82).
[260] Final Rule, *supra* note 249, at 48662, 48697, 48690 (§ 1.70007(3)–(4)).
[261] *See generally id.* at 48655–56.
[262] *Id.* at 48651 (¶ 22), 48652 (¶¶ 28–29).
[263] *See id*. at 48661–62 (¶ 77–81).
[264] *Id.* at 48664–65 (¶¶ 98–100); 47 U.S.C. § 1601 (2020).
[265] Final Rule, *supra* note 249, at 48651–52 (¶¶ 21–27).
[266] *Id.* at 48652–53 (¶¶ 28–33).

engaged in fraudulent conduct concerning national security or the Cable Landing License Act."[267]

The nature of foreign ownership of cables landing in the United States, and the use of equipment manufactured in surveillance states such as China, are valid concerns from the perspective of U.S. national security. Limiting due process protections through presumptive disqualifications is troubling for Internet governance in a time of increasingly arbitrary exercises of Executive power in the United States. This is particularly worrying in light of the extraordinarily broad provision regarding "materially false statements or . . . fraudulent conduct considering national security" provision, which potentially could apply to anyone who criticizes the President or the FCC.

D. International Cooperation or a Cable Protection Convention

The relatively weak proposals for voluntary norms in the recent OEWG and UN GGE reports reflect debates between countries such as the United States that historically have argued for a bottom-up globalized network and those such as Russia and China that have argued for greater State sovereignty over localized parts of the network.[268] So far, the U.S.-led view has carried the day. But the political dynamics are changing. China and Russia argue for extraterritoriality when it suits their desire to conduct global surveillance and stifle criticism and dissent, while the United States is increasingly viewing Internet infrastructure in territorial terms. Both trends should be resisted. Ironically, a good way to resist could involve some targeted international coordination of Internet backbone security. But any such interventions should be specific and targeted.

In particular, to mitigate the tendency towards a splinternet, the United States should work with international partners to standardize and coordinate requirements for landing stations and undersea infrastructure and to share information for monitoring and policing, including by allied naval and coast guard forces. Along these lines, some commentators have suggested the creation of an international convention for the protection of critical communications infrastructure.[269] Such proposals, however, usually go too far. They tend to ignore the historical ethos of the global open Internet, are often naïve about geopolitical competition between Russia-China and the

---

[267] *Id.* at 48653 (¶ 35).
[268] *See* Broeders & Sukmar, *Core Concerns*, *supra* note 206, at 417–18.
[269] Beckman, *Protecting Submarine Cables from International Damage*, *supra* note 123, at 290–94.

U.S.-EU blocks, and lack sensitivity to problems of censorship and surveillance in many parts of the world.

Robert Beckman, for example, suggests a cable protection convention modeled on U.N. terrorism conventions relating to hijacking and other acts against civil aviation and maritime navigation.[270] A key element of these conventions is law enforcement cooperation and extradition of offenders.[271] Beckman notes that it might be difficult to obtain momentum for this model applied to undersea Internet cables because there currently is no international agency, and no related State authorities, for coordinating undersea cables, and because of resistance from the "cable industry."[272] Beckman observes that the industry has invested billions in capital projects under a system of self-regulation and that states are not key players in industry groups, including the International Cable Protection Committee.[273] But he suggests the UN Office on Drugs and Crime (UNDOC) might be the most receptive forum for new convention on undersea cables.[274]

In fact, UNDOC is the forum for the current proposed United Nations Convention Against Cybercrime.[275] The proposed Cybercrime Convention covers traditional economic cybercrime as well as CSAM but does not contain any specific provisions regarding physical infrastructure, including undersea cables.[276] Some of the provisions of the proposed Convention—namely, those concerning economic cybercrime—could be construed to include cable damage. Article 9 requires states to adopt measures against "the damaging, deletion, deterioration, alteration or suppression of electronic data"; Article 10 requires states to adopt measures against "the serious hindering of the functioning of an information and communications technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data."[277] These provisions,

---

[270] *Id.* at 290–91.
[271] *Id.* at 291–92.
[272] *Id.* at 293.
[273] *Id.* at 294.
[274] *Id.*
[275] *See* United Nations Convention Against Cybercrime, UNODC, https://www.unodc.org/unodc/en/cybercrime/convention/home.html [https://perma.cc/R6NE-XHT2].
[276] United Nations Convention Against Cybercrime, *opened for signature* Oct. 25, 2025, G.A. Res. 79/243 (Dec. 24, 2024), https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html [https://perma.cc/T9P7-PYSP].
[277] *Id.* arts. 9–10. Both Articles require a *mens rea* of intent and further specify the element of acting "without right." *Id.* Article 13 requires measures to prohibit "[a]ny interference with

however, are clearly modeled on access, malware, and ransomware cybercrime laws. Applying them to physical damage to undersea cables would be a stretch.

More importantly, the U.N. Cybercrime Convention has attracted significant criticism because its information sharing, surveillance, and jurisdictional provisions could empower repressive States to engage in law enforcement activities on foreign soil.[278] This could include surveilling and arresting individuals on foreign soil alleged to have circumvented oppressive monitoring and censorship laws.[279]

These problems with the proposed U.N. Convention on Cybercrime highlight why suggestions like Beckman's calling for an international convention criminalizing undersea cable sabotage lack a nuanced understanding of the history and institutions of global Internet governance. The debates now roiling about the U.N. Cybercrime Treaty in some ways mirror earlier arguments about whether another U.N. body, the International Telecommunications Union (ITU), should oversee aspects of international Internet governance.[280] Notably, both in the case of the ITU and the Convention on Cybercrime, critics fear that Russia and China are attempting to use U.N. institutions to exert greater influence over the global Internet for the purpose of censorship and surveillance.[281] At the very least, any

---

the functioning of an information and communications technology system," but this Article relates only to the context of financial fraud. *Id.* art. 13.

[278] *See, e.g.*, Andrew C. Adams & Daniel Podair, *Confusion and Contradiction in the U.N. 'Cybercrime' Convention*, LAWFARE (Dec. 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention [https://perma.cc/56KF-64FU]; Karine Bannelier & Eugenia Lostri, *Is Anyone Happy With the U.N. Cybercrime Convention?*, LAWFARE (Dec. 2, 2024), https://www.lawfaremedia.org/article/is-anyone-happy-with-the-un-cybercrime-convention [https://perma.cc/9D8R-PB6P]; Eli Sher-Zagier, *The New U.N. Cybercrime Treaty is a Bigger Deal than Even Its Critics Realize*, LAWFARE (Oct. 2, 2024), https://www.lawfaremedia.org/article/the-new-un-cybercrime-treaty-is-a-bigger-deal-than-even-its-critics-realize [https://perma.cc/HC4N-UPG8].

[279] Sher-Zagier, *supra* note 278.

[280] *Civil Society Must Have a Voice as ITU Debates the Internet*, CTR. FOR DEMOCRACY & TECH. (Mar. 16, 2012), https://cdt.org/insights/civil-society-must-have-voice-as-itu-debates-the-internet/ [https://perma.cc/73FW-XSBD]; Gus Rossi, *The ITU is Trying (Again) to Govern the Internet*, PUB. KNOWLEDGE (Oct. 1, 2017), https://publicknowledge.org/the-itu-is-trying-again-to-govern-the-internet/ [https://perma.cc/XC5G-4EJN].

[281] *See e.g.,* Konstantinos Komaitis & Justin Sherman*, The ITU election pitted the United States and Russia against each other for the future of the internet*, ATL. COUNCIL (Sept. 29, 2022) https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-itu-election-and-the-future-of-the-internet/ [https://perma.cc/6747-JBHB]; Press Release,

international cybersecurity coordination regime, including for subsea cables, should include key Internet governance bodies as advisory participants, including the Internet Architecture Board (IAB), Internet Society (ISOC), and the Internet Engineering Task Force (IETF).[282]

E. A Multilayered Approach

Rather than a new international convention, a better approach would include several elements.[283] First, the customary Internet governance bodies should adopt technical standards for a global open-source subsea cable monitoring system. National authorities should require cable operators to adopt this system as part of cybersecurity requirements attached to licenses for cable landing operations.[284] Cable operators' arguments about the trade secrecy of cable locations should not prevail over this requirement. Individual cable locations generally are not hard to find in any event and claims of secrecy about this basic information are outweighed by the need for international monitoring and cooperation for the security of the global Internet. A global open-source monitoring system would better enable individual States, the international community, and civil society to identify, track, and predict (including through AI tools) threats to the infrastructure.

Second, UNCLOS should be modified to clarify that attacks on undersea Internet cables, outside the context of lawful armed conflict, are acts

---

Wyden, Merkley, Kaine, Markey, Van Hollen and Booker Warn U.N. Cyber Convention Could Justify Spying and Censorship By China, Russia and Other Authoritarian Regimes, OFFICE OF SEN. RON WYDEN (Oct. 29, 2024), https://www.merkley.senate.gov/wyden-merkley-kaine-markey-van-hollen-and-booker-warn-u-n-cyber-convention-could-justify-spying-and-censorship-by-china-russia-and-other-authoritarian-regimes/ [https://perma.cc/FN9L-S5UW].

[282] *See* INTERNET ARCHITECTURE BD., https://www.iab.org/ [https://perma.cc/9TEM-D7EZ]; INTERNET SOC'Y, https://www.internetsociety.org [https://perma.cc/6ZEL-ENP2]; INTERNET ENG'G. TASK FORCE, https://www.ietf.org/ [https://perma.cc/S8TA-G39G].

[283] *Cf.* Salgado, *supra* note 250. As Salgado notes, "[t]he US lacks a comprehensive, whole-of-government strategy to encourage investment in secure cables and has not yet built the collaborative relationship with hyperscalers that is in the interest of us all." *Id.* at 3. Salgado, however, seems less concerned about the market concentration and political influence of the hyperscalers than this Article suggests.

[284] *Cf.* DANIEL RUNDE, ERIN MURPHY & THOMAS BRYJA, CTR. FOR STRATEGIC & INT'L STUD., SAFEGUARDING SUBSEA CABLES: PROTECTING CYBER INFRASTRUCTURE AMID GREAT POWER COMPETITION 9 (2024), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816_Runde_Subsea_Cables.pdf [https://perma.cc/Y9FM-YTNT]. Runde, Murphy and Bryja argue persuasively that U.S. cable landing permitting requirements could and should be centralized and simplified. This centralization and simplification, however, should not come at the expense of weakening cybersecurity requirements attached to permits, which they do not address.

of piracy. Relatedly, the United States, NATO, and other cooperating military organizations should make the protection of undersea Internet cables against piracy and other armed attacks a more direct element of naval doctrine. In other words, there should be clear authority in international law for naval forces to protect undersea cables on the high seas in peacetime, backed by some degree of commitment to do so. Neither the United States nor any other naval force, of course, can afford to patrol Internet cable routes with any degree of consistency, but the legal authority and doctrinal commitment would provide some deterrence and facilitate a more immediate response in the event of a large-scale event.

Third, the United States should enhance financial incentives, including tax benefits, grants, and special banking relationships, for the construction of new undersea cables and the development of cable repair ship capacity.[285] The United States has engaged in such projects in the recent past. For example, the U.S. Trade and Development Agency, the U.S. Export-Import Bank, the U.S. International Development Finance Corporation, the Quad 2023 partnership, and USAID have each been involved in providing grants or financial backing for undersea cable projects connecting areas of strategic importance to the United States.[286] Since China is actively engaged in building undersea infrastructure a part of its "Digital Silk Road" initiative, U.S. parsimony in this domain would prove strategically short-sighted.[287]

Finally, antitrust and trade regulators should more carefully examine the market structure of Tier 1 Internet providers, the effects of entry into Internet backbone markets by the hyperscalers, the role of IXPs, and the terms of cable consortium and interconnection agreements. While the anecdotal evidence does not suggest any one provider possesses market power in a relevant backbone market, the high degree of concentration is concerning from an Internet governance perspective. Regulators should at least require greater public transparency and accountability regarding the cybersecurity and risk management plans of undersea cable providers.

---

[285] *Cf.* Salgado, *supra* note 250, at 18. Salgado argues that international law should allow greater scope for action of foreign cable repair vessels in territorial waters. This is a sensible recommendation, but it should also be accompanied by requirements about the identification of such vessels and the rights of States to board and inspect them in territorial waters to limit espionage or other nefarious activities under the guise of cable repair.

[286] *See id.* at 6–7, 10.

[287] *See* April A. Herlevi, *China's Strategic Space in the Digital Undersea*, NAT'L BUREAU OF ASIAN RSCH. (Mar. 2024), https://strategicspace.nbr.org/chinas-strategic-space-in-the-digital-undersea/ [https://perma.cc/2C9C-MYMK].

IV. CONCLUSION

Undersea cables are a vital but often-overlooked element of global Internet infrastructure. Recent events around the Balkan states and Taiwan demonstrate that these cables are vulnerable to physical attacks and indeed likely already have been attacked by Russian and Chinese proxies.

Cybersecurity scholars have just begun to grapple with this looming problem. Most of the existing scholarship treats the issue primarily as an international law problem, offering solutions based in the international law of the sea, the law of armed conflict, and current or future UN treaties. There are some excellent recommendations in this scholarship, particularly if existing international law is clarified and updated regarding the definition of piracy and if the United States and European navies update their doctrine to include cable protection within existing defend forward paradigms.

But the existing scholarship misses that this problem is primarily one of internet governance. Solutions based in international law— putting aside realist debates about the efficacy of international law—will not in themselves work, and in fact will quickly collide with the fundamental values of a free and open global Internet. International law therefore must coordinate with the decentralized Internet governance bodies. Those bodies should engage more closely with cybersecurity relating to the physical layer on the seabed, including through open-source cable monitoring and identification protocols.

Such protocols could be adopted into national cybersecurity policies, particularly as they apply to licenses for cable landing stations. In the United States, there is already a regulatory pathway, including current FCC rules relating to updating landing license rules, for such regulation. That regulatory pathway, however, highlights another basic tension: whether the FCC's oversight is benign or malicious depends substantially on who is overseeing the executive branch. In the past, open Internet advocates in the United States mostly cheered network neutrality rules, but those advocates failed to notice that such rules shift control over the Internet backbone from private companies to the President. Network neutrality in the United States presently is dead because of an appellate court opinion, and somewhat ironically (since net neutrality would increase Executive power), the Trump Administration's FCC will make sure it stays dead even in the unlikely event the Supreme Court revives the Biden Administration's rules. The FCC's new final rules regarding cable landing licensing could help. However, while the rules include useful cybersecurity provisions, they also suggest a focus on

unproductive culture and trade wars, which could further speed the trend towards nationalized splinternets.

Given the limited impact of international law and potential downsides of national regulatory requirements, perhaps the best policy response is to incentivize private investment in redundancy and repair capacity through tax, grant, banking, and related initiatives. Most of the Internet backbone, including undersea cables, is privately owned, resulting in no small part from the light touch regulatory approach towards broadband taken in the 1990s. The more cables there are, the less significant any one act of sabotage will be, consistent with the proverbial truth that the Internet routes around damage.

But this approach also comes at a cost to Internet governance ideals. The Tier 1 backbone provider market historically has been heavily concentrated. The greatest competition for Tier 1 providers today, including for undersea infrastructure, comes from the hyperscalers Google, Amazon, Meta, and Microsoft. It is unlikely any provider possesses or in the near term could possess significant market power in the market for operating undersea cables, but it is troubling that all of the Internet relies so heavily on so few competitors. This concern is amplified by the fact that many undersea cable deals involve consortia of multiple providers under agreements that remain opaque to the public—and the concern is heightened even more by the vital role played by IXPs in the terrestrial physical backbone, which also, particularly in the United States, often involve hidden arrangements between potential competitors.

Related to the network neutrality and landing license regulatory conundrums, this suggests a role for antitrust and trade regulators, but that role also must be constrained lest it too becomes an avenue for national authorities to control the network for protectionist or autocratic reasons under the guise of cybersecurity. In the end, there is no single solution for the tangle of undersea cable security. It will take multiple, subtly calibrated policy interventions to make some progress on this knotty problem.