Abstract

Recent disruptions to ICT infrastructure, from the Red Sea cable cuts to the devastation caused by Storm Melissa in Jamaica, illustrate the lack of any global institutional mechanism to respond to such disruptions. Policy focus over the last two decades has centred on the digital layer of communications, leaving the physical layer, such as the cables, data centres, terrestrial networks, and supply chains, without rules, institutions, or financing. This essay proposes extending the UN's new Global Mechanism on ICT security to the physical layer, through cooperation, common definitions, technical standards, and capacity support.

Safeguarding the Physical ICT Layer: A Case for Expanding the UN's Global Mechanism

In October 2025, when Storm Melissa made landfall in Jamaica, it destroyed the island's communications entirely.[1] Previously, cables were severed in the Red Sea near Jeddah, disrupting connectivity across South and West Asia.[2] Despite their widespread impact, neither incident triggered any international mechanism obliged to respond. This is partly because the policy focus over the past two decades has centred on the digital layer of communications, while the physical layer beneath it remains governed by instruments built for a different century, or not governed at all. The essay proposes extending the architecture already built for digital and cyber governance to the physical infrastructure it depends on, through shared technical definitions, a cooperative incident registry, and capacity support.

Existing Governance Landscape

The legal architecture governing physical communications infrastructure is largely a patchwork. The oldest is the 1884 Convention for the Protection of Submarine Telegraph Cables.[3] The Convention allows a warship to stop a vessel suspected of cable tampering, demand its papers, and file a report; however, the report goes to the vessel's own flag state for prosecution. Therefore, enforcement under the Convention depends on the goodwill of the very state whose vessel is under suspicion. Later, the 1958 Geneva Convention on the High Seas reinforced protections for cables but has been largely superseded by the UN Convention on the Law of the Sea (UNCLOS).[4][5]

UNCLOS, adopted in 1982, remains the most comprehensive instrument in force. It establishes that damage to cables within a state's territorial waters or exclusive economic zone falls under that state's criminal jurisdiction. However, interestingly, UNCLOS does not cover the 1884 Convention's boarding provisions but rather sits separately from it. Even UNCLOS addresses only accidental damage and criminal acts, not incidents where the cause itself is disputed. The most recent addition is the 2024 New York

---

[1] *The New York Times*, "Hurricane Melissa Live Updates," 28 October 2025, https://www.nytimes.com/live/2025/10/28/weather/hurricane-melissa-jamaica-landfall

[2] Subseacables.net, "International Cable Breaks in Red Sea Cause Latency Surge Across Asia and Gulf," 2025, https://www.subseacables.net/submarine-cables-updates/international-cable-breaks-in-red-sea-cause-latency-surge-across-asia-and-gulf/

[3] International Bureau of the Telegraph Union, *Convention for the Protection of Submarine Telegraph Cables*, Paris, 14 March 1884, https://www.loc.gov/law/help/us-treaties/bevans/m-ust000001-0089.pdf

[4] United Nations, *Convention on the High Seas*, Geneva, 29 April 1958, https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=xxi-2&chapter=21

[5] United Nations, *United Nations Convention on the Law of the Sea (UNCLOS)*, Montego Bay, 10 December 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Principles, a set of voluntary best practices for cable deployment, maintenance, and repair.[6] However, these have so far been endorsed by only a fraction of UN membership. Together, this patchwork of instruments largely protects infrastructure within national waters and provides voluntary guidance, but falls short of the governance framework required for modern communications infrastructure.

Meanwhile, the past two decades of global diplomatic effort have been almost entirely focused on the digital layer of ICT. In December 2024, the UN Cybercrime Convention became the first universal instrument on cyber matters.[7] And in July 2025, the UN's Open-Ended Working Group (OEWG) agreed to establish a permanent Global Mechanism on ICT security, which held its first session in March 2026.[8] As a result, over the years, the physical layer has lacked a comprehensive, up-to-date global framework, resulting in vulnerabilities.

Cost of the Governance Gap

Over recent years, there has been a growing number of incidents affecting ICT infrastructure. The Red Sea cable cuts in February 2024[9] and again in September 2025[10] severed multiple systems, including SMW4 and IMEWE, degrading connectivity across South Asia, West Asia, and East Africa for weeks and, at one point, affecting up to a quarter of the communication routes between Asia and Europe. The cuts occurred in a conflict zone where the Houthis were widely suspected of deliberate targeting. The group denied involvement, and the International Cable Protection Committee's early technical analysis instead pointed to a vessel's dragging anchor.[11] With no agreed way to establish the facts, the cause was never settled. The ambiguity then spread to the repair process itself. With no authoritative account of what had caused the breaks or whether the risk was ongoing, insurers had no basis to price coverage and grew reluctant to insure repair vessels in the area at all, delaying repairs by months and leaving degraded service in place far longer than the physical damage alone would have required.[12]

Cable damage on the high seas occurs far from any single state's direct observation, leaving investigators reliant on satellite tracking, vessel logs, and circumstantial timing. There is no standing body tasked with gathering that evidence, and no shared record in which findings can be logged and compared. The result

---

[6] European Commission, "The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World," 26 September 2024, https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world

[7] United Nations General Assembly, *United Nations Convention against Cybercrime*, Resolution 79/243, 24 December 2024, https://docs.un.org/en/a/res/79/243

[8] United Nations Office for Disarmament Affairs, Letter from the Chair-Designate of the Global Mechanism on ICTs in the Context of International Security, 19 March 2026, https://docs-library.unoda.org/Global_Mechanism_on_ICTs_in_the_Context_of_International_Security_-Plenary_(2026)/2026.03.19_GMech_01_Letter_from_the_Chair_Designate.pdf

[9] ComplexDiscovery, "Red Sea Cable Cuts Disrupt Connectivity and Expose Global Infrastructure Risks," 10 September 2025, https://complexdiscovery.com/red-sea-cable-cuts-disrupt-connectivity-and-expose-global-infrastructure-risks/

[10] NBC News, "Internet Disrupted as Undersea Cables Cut in Red Sea," 8 September 2025, https://www.nbcnews.com/world/middle-east/internet-disrupted-undersea-cables-cut-red-sea-internet-asia-mideast-rcna229608

[11] The National, "Cuts to Red Sea Internet Cables Were Probably Accidental, Experts Say," 9 September 2025, https://www.thenationalnews.com/future/technology/2025/09/09/red-sea-internet-cables-cut-outage/

[12] Gulf News, "Red Sea Cable Cuts: Subsea Cable Repairs Are 'Not an Easy Fix,'" 1 October 2025, https://gulfnews.com/technology/red-sea-cable-chaos-subsea-cable-repairs-are-not-an-easy-fix-1.500290675

mirrors a familiar problem from the cyber domain, where the technical signature of an attack is often well understood even when its origin is never formally attributed: what happened and who was responsible are separate questions, and the first can be established without resolving the second.[13] For physical infrastructure, neither is captured at present. The absence of any shared, authoritative record means each incident is contested in isolation.

Coming back to the example of the disruption in the Red Sea: another reason the repairs stalled was a lack of sufficient vessels and suppliers to carry them out. This is the second vulnerability that needs to be addressed. Even in areas where the cause of disruption is known and uncontested, recovery depends on a concentrated supply chain that cannot meet the demands placed on it.[14] As of now, roughly 98% of the world's undersea cables are built and installed by just four firms: the US company SubCom, France's Alcatel Submarine Networks, Japan's NEC, and China's HMN Technologies (formerly Huawei Marine). This concentration has largely resulted from state financing and backing, especially in recent years. France nationalised Alcatel, Japan plans to subsidise NEC, the US supports SubCom through fleet subsidy and diplomatic intervention, while HMN Technologies draws on Chinese state financing.[15]

Given the explicit involvement of state actors in these select players, there have been widespread concerns that their equipment could be used for espionage, interception, or sabotage, and that there is no reliable method to verify the safety of any vendor's equipment. This further reduces the pool of suitable vendors or increases the backlog for infrastructure deployment, since countries are forced to restrict vendor selection to a handful of firms based on state origin. This exclusion along state lines does not resolve the security concern it is meant to address. It simply narrows the field to vendors from friendly states rather than on any demonstrated standard. Moreover, it creates an environment in which critical infrastructure is divided along geopolitical lines, resulting in parallel systems. For example, when a consortium had provisionally agreed to let HMN Technologies build the SeaMeWe-6 cable from Singapore to Marseille at a lower cost, US pressure and the threat of sanctions shifted the contract to SubCom.[16] In the end, the displaced capacity was rebuilt as a competing parallel system by Chinese state-backed players, resulting in two networks.

Taken together, these gaps create an environment in which infrastructure protection lacks a shared means of determining what happened after an incident, and the supply chain lacks a shared means of

---

[13] American University, Center for Security, Technology, and Policy, "The Evolution of Cyber Attribution," https://www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm

[14] SubOptic Association / TeleGeography, "The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies," 2025, https://resources.telegeography.com/current-state-forecasts-submarine-cable-maintenance; Bulletin of the Atomic Scientists, "To Keep the World's Data Flowing, Countries Need to Quickly Fix Broken Undersea Cables," 30 July 2025, https://thebulletin.org/2025/07/to-keep-the-worlds-data-flowing-countries-need-to-quickly-fix-broken-undersea-cables/

[15] Daniel F. Runde et al., "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition," Center for Strategic and International Studies (CSIS), August 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

[16] Lightreading, "US Hardball Drove Chinese Vendor from Huge Cable Project," November 2023, https://www.lightreading.com/cable-technology/us-hardball-drove-chinese-vendor-from-huge-cable-project-reports; Reuters/US News, "China Plans $500 Million Subsea Internet Cable to Rival US-Backed Project," April 2023, https://www.usnews.com/news/world/articles/2023-04-06/exclusive-china-plans-500-million-subsea-internet-cable-to-rival-u-s-backed-project

determining what is safe to build in the first place. The absence of a global framework has forced a unilateral approach to physical ICT infrastructure, despite its inherently global and interdependent nature.

The gaps described so far, whether in the means of incident reporting or the common standards for trusting equipment networks, disproportionately affect the states with the least capital and institutional resources. India is a clear case study. It hosts 20% of global internet traffic but only 2% of global subsea traffic. The majority of its international cables land within a single six-kilometre stretch of coast near Mumbai, and close to 60% of its international traffic routes through one corridor running past the Red Sea and the Gulf. It also doesn't own a cable-repair vessel. When the Red Sea cuts of February 2024 struck, India waited on repairs not only because of the broader security situation, but because the backlog for Indian Ocean repairs stretched into months.[17]

The situation is even starker for countries with fewer resources and connectivity. When a volcanic eruption in 2022 severed the only cable connecting Tonga to the rest of the world, the island spent roughly five weeks in near-total digital isolation. Tonga had to wait over a year for a replacement cable to be manufactured and shipped from France before its domestic cable could be fixed.[18] These states are also disproportionately affected by supply chain constraints mentioned earlier. They are forced to exclude vendors judged untrustworthy on security grounds, yet unable to match the financing and speed those vendors offered.

The frameworks that do exist were largely shaped by the states least likely to face these conditions and are not adequately equipped to close these gaps for those who are. And the concerns extend beyond equity and fairness. A network is only as resilient as its weakest node: the exposed states carry traffic, host supply routes, and their outages ripple outward into the systems everyone else depends on. Any response, therefore, must be inclusive and global in nature, built on consensus rather than on the capacity of individual states to act alone.

Proposal: Extending the Global Mechanism

So how should the gaps be closed? The cleanest solution, at least on paper, would be to build a dedicated institutional mechanism for physical infrastructure. However, a standalone global mechanism would likely mean prolonged negotiations with no guarantee of success. It would also make little sense to separate the governance of the physical layer from the digital one. Whether a network is disrupted by a severed cable or a cyberattack, the end result is very much the same, and so should be its governance. Lastly, two parallel institutions, each governing one layer, would invite duplication, jurisdictional confusion, and competition for the scarce diplomatic bandwidth.

---

[17] The Industry Outlook, "Is Digital Lifeline of India at Risk? The Undersea Cable Chokepoints," May 2026, https://www.theindustryoutlook.com/machinery-and-equipment/panorama/is-digital-lifeline-of-india-at-risk-the-undersea-cable-chokepoints-nwid-17400.html; Communications Today, "Beneath the Boom: The Subsea Cable Contradictions Defining India's Digital Future," June 2026, https://www.communicationstoday.co.in/beneath-the-boom-the-subsea-cable-contradictions-defining-indias-digital-future/; Bridge India, "How India's Undersea Internet Cables Lie Exposed," April 2026, https://bridgeindia.substack.com/p/how-indias-undersea-internet-cables

[18] Al Jazeera, "Tonga Internet Reconnected Five Weeks After Volcanic Eruption," 23 February 2022, https://www.aljazeera.com/news/2022/2/23/tonga-internet-reconnected-five-weeks-of-volcanic-eruption; Data Center Dynamics, "Tonga's Domestic Submarine Cable Fixed 18 Months After Volcanic Eruption," 14 July 2023, https://www.datacenterdynamics.com/en/news/tongas-domestic-submarine-cable-fixed-18-months-on-from-volcanic-eruption/

Therefore, the path of least resistance would be to build on a mechanism that already exists. In July 2025, after decades of ad hoc and time-limited processes, UN member states agreed by consensus to establish the Global Mechanism on ICT security, making it the first permanent UN body of its kind. Its structure, from the annual plenary to the dedicated thematic groups, already covers the protection of digital critical infrastructure, and it operates a Global Points of Contact Directory through which states share information about incidents. Given that the most difficult stage of reaching consensus to create such a body has already been completed, extending the Mechanism's mandate to cover physical communications infrastructure, or establishing a dedicated track formally linked to it, is the natural next step. Its technical work can also draw on existing bodies such as the ITU's International Advisory Body for Submarine Cable Resilience, feeding specialist expertise into the political process.[19]

Working on this, the first task would be to ensure consensus on definitions, thereby laying the foundation for the broader governance framework. At present, there is no common definition of protected communications infrastructure. The existing instruments cover only cables and barely include the broader ecosystem of data centres, internet exchange points, landing stations, and the terrestrial backbone. What is required is a common classification of the physical assets that constitute critical communications infrastructure, and of the categories of disruption that threaten them. This would also, hopefully, be the least contentious element of the framework, since no party is asked to accept a constraint on its conduct. Without these universal definitions, states would struggle to coordinate protection efforts, and no other instruments, such as an incident registry or technical standards, would be possible.

Second, regarding incident reporting, any proposed registry would need to be practical rather than aspirational and focus on what can be achieved through consensus. An incident registry, housed within the Global Mechanism's existing Points of Contact Directory, would allow states and operators to log the physical facts of an incident: what was damaged, where, when; the probable physical cause, where it can be established; the time taken to repair; and the cost. Policymakers would need to resist the temptation to assign responsibility, name a culpable state, or issue a finding of fault. As in the cybersecurity space, attribution is a political act, and states would likely resist any international body that performed it on their behalf. The registry should therefore record only what happened, not who is to blame. This not only ensures consensus among member states but also serves the interests of the very states most likely to be wary of it. A shared record lets insurers price risk, which over time lowers repair-coverage costs. It lets exposed states learn from one another's repair experience, which compounds over time. Lastly, it directs help to where the data shows it is most needed.

Third, and lastly, the mechanism should offer solutions to the supply chain problems raised earlier. The first was trust. As noted, the lack of any common way to verify that a vendor's equipment is safe has led states to use origin as a proxy. The answer is to build a common, internationally agreed framework for certifying the security of communications equipment, open to any vendor, regardless of origin, and administered by the same multilateral body. The model already exists in the cybersecurity field, where the Common Criteria allow products to be evaluated against agreed technical requirements rather than the reputation of the state that produced them.[20] This addresses the security concern directly, and it lets

[19] International Telecommunication Union, "International Advisory Body for Submarine Cable Resilience," established November 2024, https://www.itu.int/digital-resilience/submarine-cables/advisory-body/

[20] Common Criteria Recognition Arrangement (CCRA), "Common Criteria for Information Technology Security Evaluation," https://www.commoncriteriaportal.org/

the market compete on merit rather than fracture along blocs. In keeping with the emphasis on practicality, the standard should be a voluntary technical baseline and not override any government's right to make its own security decisions.

The second supply chain issue was recovery. Even when the cause of a fault is uncontested, the states most exposed wait the longest, given their lack of resources and institutions. Here the precedent already exists within the UN's own system. The UN Humanitarian Response Depots pre-position relief supplies at shared hubs so they can be dispatched wherever disaster strikes, rather than each agency maintaining its own. A repair arrangement would do the same for vessel capacity, pooling ships so that a break receives the nearest available vessel rather than waiting in one operator's queue while another's network stays dark. It would be supported by a dedicated resilience-financing window, modelled on the Central Emergency Response Fund, to release emergency funds within hours of a crisis.[21]

Addressing the Counter-Arguments

A proposal of this kind would invite several reasonable arguments against it. The first would be that major powers and blocs would be reluctant to agree to such a framework. But recent history, illustrated by the Global Mechanism, shows that states, while disagreeing over how far international law should constrain their conduct, continue to accept the need for a common institution and a shared agenda. The proposal, recognising that consensus is a precondition for sustainable progress, draws on this history.

The second likely argument would be the inverse of the first: that a consensus-based mechanism would be too slow and ineffective, and that any meaningful progress would instead come from select arrangements. There is truth here. The efforts already underway, such as the QUAD's Pacific cable commitments[22] or the EU's action plan[23], have seen real progress in a shorter time than any universal process will. But this has also produced a multi-tiered form of preparedness, fracturing the world into multiple blocs. In an interdependent network, where the vulnerability of the weakest nodes propagates to everyone, blocs cannot substitute for a universal mechanism.

The third likely argument is that no technical certification can ever fully guarantee a vendor's equipment is safe, and that a determined state-linked supplier might find a loophole in any audit. This too is correct: a shared standard does not eliminate risk completely. But the relevant comparison is not with perfect security (there is no such thing) but with the present alternative, in which trust is assigned by nationality proxy rather than by any technical and independent examination. A standard that can be met, audited, and improved over time is a better start than a national proxy.

The last argument, and the most legitimate, is an institutional concern. The Global Mechanism, still new and already criticised for the breadth of its agenda, risks being overloaded by the addition of physical

---

[21] UN World Food Programme, "UN Humanitarian Response Depot (UNHRD) Network," https://www.unhrd.org/; UN Office for the Coordination of Humanitarian Affairs, "Central Emergency Response Fund (CERF)," https://cerf.un.org/

[22] White House, "Fact Sheet: 2024 Quad Leaders' Summit," 21 September 2024, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/09/21/fact-sheet-2024-quad-leaders-summit/

[23] European Commission and High Representative, "EU Action Plan on Cable Security," 21 February 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025JC0009

infrastructure.[24] But this argument only reinforces the need for proper debate and deliberate design. The alternative of a separate institution is impractical, if not worse, for the reasons set out earlier. The only viable solution is to consolidate work under a single mechanism rather than fragmenting it. Taken together, these objections confirm the argument that any proposal must be rooted in practicality.

Conclusion

The physical layer on which all communication depends has been left to a makeshift set of rules fragmented along geopolitical lines, even as the threats to it have become deliberate and transnational. No institution is responsible for it as a whole, and so its vulnerability falls hardest on the states least able to bear it and, through them, on everyone. The solution need not be invented from nothing. The world has just built its first permanent, universal body for the security of communications technologies; extending its reach to the physical infrastructure beneath the digital layer is the obvious choice.

AI Acknowledgment

This essay was developed by the author. Limited assistance was obtained using Claude by Anthropic for spelling and grammar checks, improving clarity, feedback and identifying publicly available sources for further research. Grammarly was also used for suggestions on spelling and grammar. The analysis, arguments, structure, evidence, and conclusions are the author's own, and the final submission is substantially the entrant's own original work.

[24] Global Partners Digital, "The OEWG Ends and a New UN Cybersecurity Permanent Mechanism Is Born," 24 July 2025, https://www.gp-digital.org/the-oewg-ends-and-a-new-un-cybersecurity-permanent-mechanism-is-born/