IIC Future Leaders Competition 2026

Resilience by Accident, Not by Design

Are Current Policies Enough to Protect Communications Networks from Disruption?

Theme: Effective emergency preparedness: safeguarding ICT systems and infrastructure from disruption

Submitted to the International Institute of Communications

2026

Table of Contents

Abstract 3
1. Introduction 3
2. A Policy Regime Built in the Rubble 3
3. Protecting the Infrastructure 4
Undersea cables 4
Terrestrial networks and the single point of failure 5
Data centres and the power dependency 5
4. Diversifying the Supply Chain 5
5. Are Current Policies Sufficient? 6
6. What More Is Needed, and How 7
7. Conclusion 7
References 8

Abstract

Communications networks are treated as critical national infrastructure, yet the policies meant to protect them have largely been written after a failure rather than ahead of one. Drawing on the 2025 Red Sea cable cuts, Hurricane Melissa's devastation of Jamaica, and Canada's 2022 Rogers outage, this essay argues that current network-resilience policy is necessary but structurally insufficient. Three weaknesses recur across jurisdictions: a reactive posture that responds to incidents instead of preventing them; a siloed governance model that separates physical security, cyber security, supply-chain integrity, and power dependency; and an over-reliance on voluntary commitments from operators. Examining both infrastructure protection (undersea, terrestrial, and data-centre) and supply-chain diversification, the essay weighs the case for restraint against the evidence of fragility, and proposes a shift toward resilience that is designed in from the start, integrated across domains, adequately funded, and enforceable in practice.

1. Introduction

On 6 September 2025, several submarine cables in the Red Sea were severed near Jeddah, most likely by a ship's anchor dragging across the seabed in the Bab el-Mandeb Strait. Internet performance degraded across India, Pakistan, the Gulf, and parts of Africa, and even Microsoft's Azure cloud platform was forced to reroute traffic (Subsea Cables, 2025; Capacity Media, 2025). Seven weeks later, Hurricane Melissa made landfall in Jamaica as a Category 5 storm and knocked out power and internet for roughly three-quarters of the island, with as much as 70 percent of the mobile network offline in the immediate aftermath (The New York Times, 2025; Jamaica Observer, 2026). The causes were very different, one a likely accident at sea and the other a record-breaking natural disaster, yet they produced the same lesson: the systems on which modern societies most depend in an emergency are the very systems most likely to fail during one.

The International Telecommunication Union defines network resilience as the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation, based on prepared facilities (International Telecommunication Union, 2014). That last phrase carries most of the weight. Submarine cables alone carry an estimated 97 percent of intercontinental internet traffic and underpin trillions of dollars in daily financial transactions (European Council on Foreign Relations, 2025), and yet much of the policy architecture protecting them has been assembled reactively, one incident at a time.

This essay argues that the policies currently designed to protect national and international communications systems from disruption are necessary but insufficient. They are insufficient not because regulators have done nothing. They have in fact done a great deal. They fall short because the prevailing approach is reactive rather than preventive, fragmented across institutional silos, and dependent on the goodwill of commercial operators. Focusing on the two policy areas at the heart of network resilience, the protection of infrastructure and the diversification of the telecommunications supply chain, the essay sets out where current policy falls short and how it might credibly be strengthened.

2. A Policy Regime Built in the Rubble

The defining characteristic of contemporary resilience policy is that it tends to arrive after the disruption it is meant to prevent. Canada offers an unusually clear example. On 8 July 2022, a configuration error during a network upgrade triggered a national Rogers outage that left millions of customers without service for up to fifteen hours, disabling access to 9-1-1, emergency alerting, and electronic payment systems (CRTC, 2022). The regulatory response followed the failure. Within days the government directed carriers to negotiate a formal agreement on emergency roaming, mutual assistance, and public communications, and in September 2022 twelve telecommunications service providers signed a memorandum of understanding on reliability (Government of Canada, 2022). More than three years later, in 2025, the regulator finalised rules requiring providers to notify authorities within two hours of a major outage and to explain what went wrong (CBC News, 2025).

The same pattern holds internationally. NATO launched its Baltic Sentry surveillance mission in January 2025 only after a series of suspected sabotage incidents against Baltic Sea cables, and the European Union published its Action Plan on Cable Security the following month (European Commission & High Representative, 2025). Each measure is sensible. But a policy regime that activates in response to the last crisis is, by its nature, one step behind the next one. Reaction is not the same as readiness.

3. Protecting the Infrastructure

Undersea cables

Subsea cables are at once the backbone of global communications and one of its most exposed components. They are thin, they lie largely unguarded on the seabed, and they pass through a handful of geographic chokepoints. The Red Sea cuts showed both the fragility and, importantly, a degree of built-in resilience: automatic rerouting kept much traffic flowing, albeit more slowly, because the system retained redundant paths (ThousandEyes, 2025). That redundancy, however, is unevenly distributed. Well-connected hyperscalers rerouted within a day, while regions and operators dependent on a small number of cables did not have that luxury.

Two structural problems compound the exposure. The first is that repair capacity is scarce. The global fleet of specialised cable-repair vessels is small and ageing, and the median time to repair a fault is estimated at around forty days, longer still when weather, access restrictions, or simultaneous incidents intervene (EU Blue Economy Observatory, 2026; Atlas Institute for International Affairs, 2026). The second is that jurisdiction is murky. Most cables lie in international waters, where the United Nations Convention on the Law of the Sea offers only thin tools to deter or prosecute interference, and attribution is often difficult to establish quickly. The Red Sea cuts were probably accidental, but the Baltic Sea has seen a run of suspected deliberate incidents. These include damage to the C-Lion1 and BCS East-West cables in late 2024, and the Eagle S tanker, which was linked to a Gulf of Finland cable break on Christmas Day 2024 (European Commission & High Representative, 2025; Atlas Institute for International Affairs, 2026). All of this sits against a backdrop of reports that adversaries are developing purpose-built

deep-sea cable-cutting capabilities (European Council on Foreign Relations, 2025). The same physical asset can be threatened by an anchor, a hurricane, or a hostile state, which is why a resilience policy organised around any single threat will miss the others.

Policy is beginning to respond. The EU's Action Plan organises its work around prevention, detection, response and recovery, and deterrence. NATO's Baltic Sentry mission, launched in January 2025, added frigates, patrol aircraft, and naval drones to raise the cost of sabotage (Carnegie Endowment for International Peace, 2025). In February 2026 the European Commission announced a €347 million package and a Cable Security Toolbox, which includes a pilot to pre-position modular repair equipment in Baltic ports (EU Blue Economy Observatory, 2026). These are meaningful steps. Yet they remain heavily weighted toward detection and surveillance rather than deterrence and rapid repair, and the underlying shortage of repair vessels is barely addressed. Those vessels are a capital-intensive public good that the market under-provides. The EU's own expert group has warned that traditional European operators now own only about 2 percent of transatlantic cable capacity, with much new capacity financed by non-European hyperscalers, deepening a dependency that resilience policy has not yet confronted (Atlas Institute for International Affairs, 2026).

Terrestrial networks and the single point of failure

The Rogers outage exposed a different vulnerability, not a severed cable but a brittle internal architecture. An independent assessment found that the company's wireless and wireline cores were insufficiently separated, so a single fault cascaded across both, and that staff could not even remotely access network elements to diagnose the problem (CRTC, 2023). The government framed its response around three pillars: robust networks and systems, coordinated planning and preparedness, and strengthening accountability (Government of Canada, 2022). It also tasked a security advisory committee with developing further measures. The concrete results, however, were a mandatory outage-notification rule and a mutual-assistance memorandum that was itself signed at the industry's own table. Both improve transparency and coordination once a failure has occurred. Neither does much to compel the architectural choices, such as core separation and route diversity, that would prevent the failure in the first place. The strongest pillar, accountability, is also the one that has advanced least. A memorandum among competitors is not the same as an enforceable obligation with consequences for breach.

Data centres and the power dependency

Hurricane Melissa illustrated a third dimension that is too often treated separately: communications resilience is inseparable from power resilience. Cell towers failed not only from wind damage but because backup generators were depleted within the first two days, producing what analysts described as a cascading infrastructure failure (Direct Relief, 2025). Data centres concentrate this risk further, bundling computing, storage, and connectivity into single physical sites with intense power and cooling demands. A resilience policy that addresses networks while ignoring the energy systems they sit on top of is protecting only half the chain.

4. Diversifying the Supply Chain

The second pillar of resilience, supply-chain diversification, has become entangled with national security, and the two objectives sometimes pull against each other.

The starting point is concentration. Five vendors (Huawei, Ericsson, Nokia, Samsung, and ZTE) account for roughly 94 percent of the global radio-access-network market (Mordor Intelligence, 2026). When governments exclude vendors designated as high-risk, they reduce one risk while sharpening another. Canada's 2022 decision to bar Huawei and ZTE, which required removal of their 5G equipment by mid-2024 and their 4G equipment by the end of 2027, mirrored moves by its Five Eyes allies (The Register, 2022) and came with amendments making security an overriding objective of telecommunications policy (Public Safety Canada, 2023). But removing two suppliers from a market of five can leave operators dependent on what is effectively a two-vendor field for macro radio equipment, substituting a foreign-control risk for a market-concentration risk that is itself a resilience hazard.

In fairness, the security rationale for the bans was substantial. Governments concluded that a supplier which could be compelled to follow the directions of a foreign state has no place in critical national infrastructure, and that judgement is defensible even at a commercial cost. The difficulty is that exclusion and diversification are different projects, and pursuing the first without delivering the second leaves networks more concentrated, not less.

The favoured policy answer is Open RAN, which disaggregates network components so that hardware and software from different suppliers can interoperate. The United Kingdom has invested £250 million in Open RAN, run trials with new entrants such as NEC, and signalled the market further by committing to sunset its legacy 2G and 3G networks (UK Government, 2024). The United States has committed roughly USD 1.5 billion through a public wireless supply-chain innovation fund (Mordor Intelligence, 2026). The logic is sound, but the commercial reality is unforgiving. Incumbents have responded by offering their own nominally "open" products, and flagship deployments such as AT&T's agreement with Ericsson have effectively become single-vendor arrangements that blunt the diversification purpose (CMS, 2025). The telecommunications-equipment market contracted by about 11 percent in 2024, its sharpest decline in two decades, leaving even the established vendors financially strained (Telco Magazine, 2025). Diversification is being attempted in a shrinking market with little headroom for new scale entrants, a structural obstacle that subsidies alone have not overcome. Canada, for its part, has been more active on exclusion than on the affirmative and costly work of cultivating alternative suppliers.

5. Are Current Policies Sufficient?

The honest answer requires engaging the strongest case for the defence. Several arguments suggest that current policy is broadly adequate. The Red Sea episode showed that designed-in redundancy works, since the internet rerouted itself and did not collapse. Markets arguably self-correct, as operators who suffer outages invest in resilience to protect their reputations. Jamaican carriers, for

instance, moved quickly to rebuild fibre backbones and reduce reliance on single routes after Melissa (Jamaica Observer, 2026). Mandatory resilience standards impose real costs, can slow network roll-out, and risk entrenching incumbents who can best afford compliance, while heavy-handed vendor restrictions raise prices and may sacrifice the most advanced technology. There is a legitimate argument that regulators should set outcomes and let competitive operators choose how to meet them.

These points have force, and good policy should take the cost and innovation concerns seriously rather than dismiss them. But they do not rescue the sufficiency claim. Redundancy held for the well-connected and failed the vulnerable. Resilience that protects cloud platforms while leaving an entire island population offline is not resilience in any policy-relevant sense. Market self-correction is real, but it is slow, partial, and biased toward commercially valuable routes rather than socially essential ones. And the recurring structure of the policy response is familiar: react to an incident, convene the industry, secure a voluntary undertaking, and add a reporting requirement. That sequence addresses visibility and coordination far better than it addresses prevention. Three gaps persist across jurisdictions. Policy is reactive rather than preventive. It is siloed, treating physical security, cyber threats, supply-chain integrity, and power dependency as separate files. And it leans on voluntary commitments that lack the bite to change behaviour before a crisis. On the central question, current policies are a necessary foundation, but they are not enough.

6. What More Is Needed, and How

Five shifts would move policy from reaction toward readiness, while respecting cost and market realities.

First, move from notification to prevention through resilience-by-design standards. Rather than only requiring operators to report failures, regulators should require demonstrable architectural resilience, including core separation, route and supplier diversity, and minimum power-autonomy thresholds for critical sites. To avoid crushing smaller providers, the obligations should be risk-based and proportionate, scaling with an operator’s size and the criticality of the population it serves.

Second, treat repair and recovery capacity as a strategic national asset. The shortage of cable-repair vessels and pre-positioned equipment is a public-good problem the market will not solve alone. Regional reserve fleets and stockpiles of modular repair kit, on the model of the EU’s Baltic pilot, should be funded through public-private partnership and coordinated across allied states, because no single country can justify the standing cost.

Third, integrate governance across domains. The Melissa and Rogers cases show that physical, cyber, supply-chain, and power risks converge in the same incident, yet they are typically owned by different agencies. A single accountable resilience function, or at the very least a binding coordination mandate linking the communications regulator with security and energy authorities, would close the seams that disruptions exploit.

Fourth, make commitments enforceable. Voluntary memoranda and good-faith undertakings are a reasonable first step, but resilience obligations need credible consequences for non-compliance, comparable to the administrative monetary penalties already used in other areas of communications and anti-fraud regulation. A penalty regime need not be punitive to be effective. Its purpose is to price the cost of under-investing in resilience so that prevention becomes the rational commercial choice rather than a discretionary one. Enforcement is what turns a paper commitment into an engineered outcome, and without it prevention remains optional and tends to lose to short-term cost pressure.

Fifth, fund diversification honestly and internationally. Excluding high-risk vendors without building alternatives simply concentrates the market. Sustaining a third or fourth scale vendor will require subsidy, guaranteed demand, and interoperability mandates. Given the small size of any one national market, it will also require coordinated procurement among allied states to pool enough demand to make new entry viable. Satellite direct-to-cell services, which provided a lifeline in Jamaica (Data Center Dynamics, 2025), should be embraced as a complement to terrestrial resilience, though treated with caution given their own emerging concentration in a handful of providers.

7. Conclusion

Communications networks are the infrastructure on which every other emergency response depends. When they fail, the tools to coordinate rescue, restore power, and reassure families fail with them. The policies now in place are a serious and necessary foundation: mandatory outage reporting, mutual-assistance agreements, cable-security action plans, vendor restrictions, and diversification funds. But almost all of them were built in the rubble of a previous failure, and they remain reactive, fragmented, and reliant on voluntary compliance. The Red Sea cuts, Hurricane Melissa, and the Rogers outage were not anomalies. They were previews. The cost of designing resilience in advance is far smaller than the cost of the next disruption, and it calls for preventive standards, strategic repair capacity, integrated governance, enforceable obligations, and honestly funded diversification. The task for policymakers is to make resilience a property that is designed into communications systems, not one discovered by accident after they break.

References

Atlas Institute for International Affairs. (2026, April 12). *The silent front: Cable crisis in the Baltic Sea*. https://atlasinstitute.org/the-silent-front-cable-crisis-in-the-baltic-sea/

Canadian Radio-television and Telecommunications Commission. (2022, July 12). *Statement by Ian Scott, Chairperson and CEO of the CRTC, regarding Rogers' outage*. Government of Canada. https://www.canada.ca/en/radio-television-telecommunications/news/2022/07/

Canadian Radio-television and Telecommunications Commission. (2023). *Assessment of Rogers networks for resiliency and reliability following the 8 July 2022 outage* (Xona Partners report). https://crtc.gc.ca/eng/publications/reports/xonarp2023.htm

Capacity Media. (2025, September 9). *Ship likely cut subsea cables in the Red Sea, disrupting connectivity across three continents*. https://www.capacitymedia.com/article/red-sea-connectivity

Carnegie Endowment for International Peace. (2025, June 5). *The Baltic Sea at a boil: Connecting the shadow fleet and episodes of subsea infrastructure sabotage*. https://carnegieendowment.org/research/2025/06/baltic-russia-maritime-cable-sabotage

CBC News. (2025, September 4). *Telecom outages will need to be reported and explained under new rules, CRTC says*. https://www.cbc.ca/news/business/telecom-outages-crtc-rules-1.7625283

CMS. (2025, March 13). *What is happening to Open RAN?* https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/what-is-happening-to-open-ran

ComplexDiscovery. (2025, September 10). *Red Sea cable cuts disrupt connectivity and expose global infrastructure risks*. https://complexdiscovery.com/red-sea-cable-cuts-disrupt-connectivity-and-expose-global-infrastructure-risks/

Data Center Dynamics. (2025, October 29). *Telecoms connectivity plummets in Jamaica following Hurricane Melissa, as Starlink provides direct-to-cell coverage*. https://www.datacenterdynamics.com/en/news/

Direct Relief. (2025, November 4). *Using technology to measure power outages, critical infrastructure damage after Hurricane Melissa*. https://www.directrelief.org/2025/11/

Emergency Telecommunications Cluster. (2025). *Caribbean: Hurricane Melissa*. https://etcluster.org/emergency/caribbean-hurricane-melissa

EU Blue Economy Observatory. (2026, February 11). *€347 million to protect Europe's submarine cables*. European Commission. https://blue-economy-observatory.ec.europa.eu/

European Commission & High Representative. (2025, February). *Joint communication: EU action plan on cable security* (CELEX 52025JC0009). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009

European Council on Foreign Relations. (2025, July 9). *Shallow seas and "shadow fleets": Europe's undersea infrastructure is dangerously vulnerable*. https://ecfr.eu/article/shallow-seas-and-shadow-fleets-europes-undersea-infrastructure-is-dangerously-vulnerable/

Global News. (2022, July 11). *Rogers outage: CRTC to investigate "root cause" of network failure*. https://globalnews.ca/news/8981259/rogers-outage-crtc-investigation

Government of Canada. (2022, September 7). *Statement from Minister Champagne on Canada's telecommunications reliability agenda following Rogers' outage on July 8, 2022*. https://www.canada.ca/en/innovation-science-economic-development/news/2022/09/

International Telecommunication Union. (2014). *Disaster relief systems, network resilience and recovery* (ITU-T Focus Group Technical Report T-FG-DRNRR-2014-6). https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-DRNRR-2014-6-PDF-E.pdf

Jamaica Observer. (2026, March 25). *Telecoms rebuild networks after storm but warn policy delays slowing roll-out*. https://www.jamaicaobserver.com/2026/03/25/telecoms-rebuild-networks-storm-warn-policy-delays-slowing-roll/

Mordor Intelligence. (2026, January 19). *Open RAN market size, growth, share & industry trends*. https://www.mordorintelligence.com/industry-reports/open-ran-market

The New York Times. (2025, October 28). *Melissa devastates Jamaica as officials assess destruction*. https://www.nytimes.com/live/2025/10/28/weather/hurricane-melissa-jamaica-landfall

Public Safety Canada. (2023). *Parliamentary committee notes: Telecommunications Act amendments and 5G security*. https://www.publicsafety.gc.ca/

The Register. (2022, May 20). *Canada bans Huawei and ZTE from 5G networks*. https://www.theregister.com/2022/05/20/canada_bans_huawei_and_zte/

Subsea Cables. (2025, September 8). *International cable breaks in Red Sea cause latency surge across Asia and Gulf*. https://www.subseacables.net/submarine-cables-updates/international-cable-breaks-in-red-sea-cause-latency-surge-across-asia-and-gulf/

Telco Magazine. (2025, September 17). *Global telecom vendors face market shake-up in 2024*. https://telcomagazine.com/news/global-telecom-vendors-face-market-shake-up-in-2024

UK Government. (2024). *Telecoms supply chain diversification: Independent report and recommendations* (Telecoms Supply Chain Diversification Advisory Council). https://assets.publishing.service.gov.uk/

Claude AI, Model Sonnet 4.5. I used it to find sources, verify the sources, target the structure of sentences that were incorrect or weak, and ensure that the essay with the IIC criteria. I wrote the text myself.