IIC FUTURE LEADER'S COMPETITION 2026

Emergency Preparedness

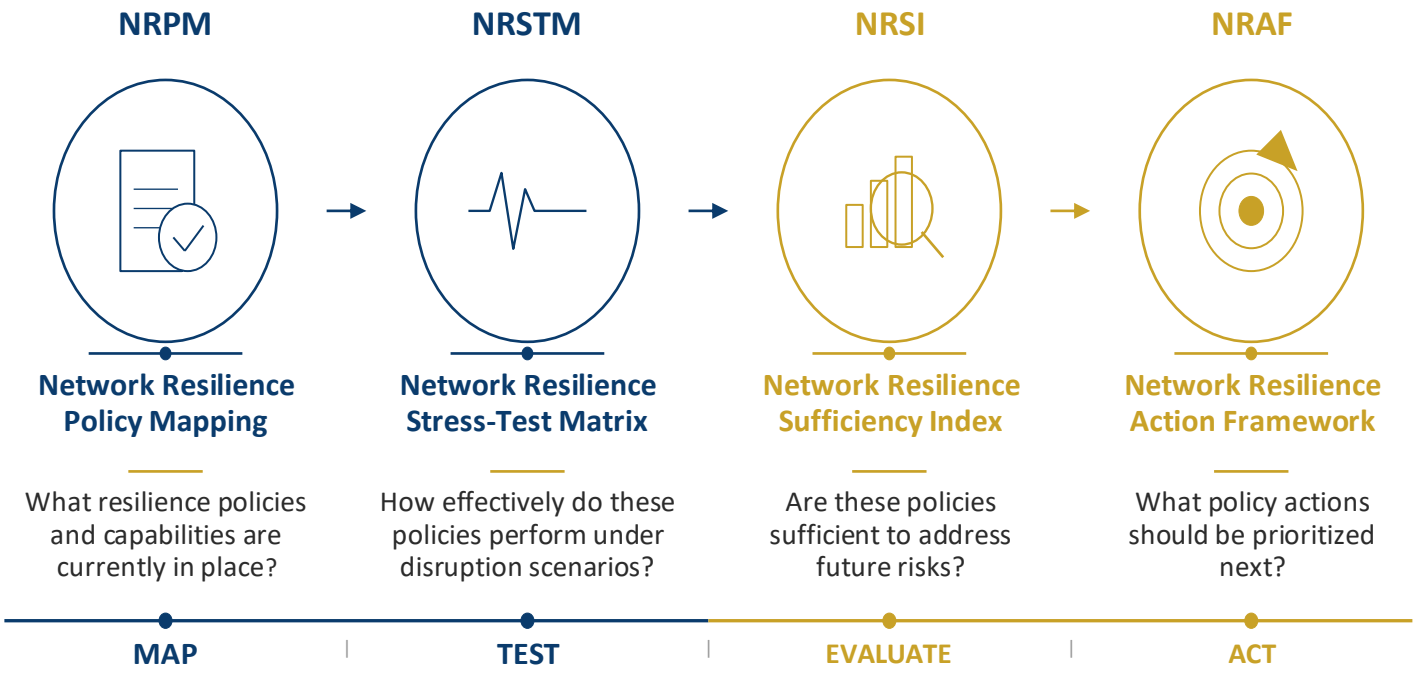
Are Existing Resilience Frameworks Sufficient for Tomorrow's Risks?

"A Framework-driven Essay on Effective Emergency Preparedness: A Four-Stage Solution for Communications Resilience"

Author's Analytical Framework

An **Original Analytical Framework** developed by the author for the **IIC Future Leaders Competition 2026** to provide strategic analysis and actionable solutions

A four-stage framework for assessing ICT network resilience and guiding strategic policy action.



Framework-Driven Essay on Effective Emergency Preparedness

A Four-Stage Solution for Communications Resilience

ABSTRACT

Communications networks are **critical infrastructure**, yet their resilience faces challenges from an evolving risk landscape. This paper introduces the author's four-stage framework—**Network Resilience Policy Mapping (NRPM), Network Resilience Stress-Test Matrix (NRSTM), Network Resilience Sufficiency Index (NRSI), and Network Resilience Action Framework (NRAF)**—to evaluate whether current policies adequately safeguard ICT infrastructure.

The assessment examines two policy pillars: **infrastructure protection** (undersea cables, telecommunications networks, and data centres) and **supply chain diversification** (equipment vendors, semiconductors, cloud infrastructure, software supply chains, and Open RAN).

The analysis finds that **protection and governance frameworks are relatively mature, while supply chain diversification remains the most significant resilience gap**. It identifies **submarine cable resilience, cloud concentration, semiconductor supply chains, and international coordination** as the most critical vulnerabilities.

The paper concludes with a sequenced policy action framework to strengthen long-term ICT resilience and preparedness.

Analytical Methodology

The four-stage framework moves from diagnosis to prescription — **mapping current capabilities (NRPM**), **testing them against real disruptions (NRSTM), assessing forward adequacy (NRSI**), and **translating findings into sequenced action (NRAF**). Each stage builds upon the last, ensuring that policy recommendations are grounded in both historical evidence and future risk trajectories.

01	02	03	04
NRPM	**NRSTM**	**NRSI**	**NRAF**
Network Resilience Policy Mapping	**Network Resilience Stress-Test Matrix**	**Network Resilience Sufficiency Index**	**Network Resilience Action Framework**
Baseline capability inventory	*Performance under real disruptions*	*Forward adequacy assessment*	*Prioritised policy interventions*

METHODOLOGICAL NOTE

A Note on Scoring Methodology

Scores throughout this paper — across the **NRPM, NRSTM, and NRSI** frameworks — reflect the **author's own qualitative judgement**, informed by the cited policy documents, standards, and case evidence rather than a standardised third-party rubric or independently audited scoring instrument. No formal inter-rater reliability testing was conducted. The scores should therefore be read as a structured, transparent expression of the author's analytical assessment — intended to support comparative reasoning across policy areas — rather than as precise or independently verifiable measurements**. Readers are encouraged to consult the underlying sources cited in the Bibliography to form their own judgements.**

A single network disruption can affect millions of people within minutes, disrupting hospital coordination, emergency response, and financial services simultaneously (United Nations, 1998; ISO, 2019). In an era of deepening digital interdependence, communications infrastructure has become fundamental to economic activity and public safety. Yet many policies designed to protect it were shaped for a different technological and risk landscape.

Recent events have shown this mismatch clearly. The 2024 Red Sea cable disruptions revealed the fragility of international undersea connectivity (Carnegie Endowment for International Peace, 2024). Storm Melissa in Jamaica showed how a single severe weather event can sever communities from their only communications lifeline (UNDRR, 2015). The CrowdStrike global outage demonstrated that one flawed software update can cascade across critical services worldwide, by passing conventional physical protections (NIST, 2022). Likewise, the COVID 19 semiconductor crisis highlighted how shortages of the chips underpinning modern networks can emerge within months rather than years (Semiconductor Industry Association, 2024).

Together, these events illustrate a fundamental shift in the emergency preparedness challenge. Safeguarding communications is no longer solely about hardening physical infrastructure.

It also requires ensuring service continuity across interconnected digital, industrial, and geopolitical ecosystems (World Economic Forum, 2024). This paper examines this gap through a four-stage methodology aligned with the competition's two principal policy areas.

Accordingly, the analysis is structured around two policy pillars: **(i)** protecting critical communications infrastructure, including undersea cables, telecommunications networks, and data centers, and **(ii)** diversifying the telecommunications supply chain, covering vendors, semiconductors, cloud services, and Open RAN.

Each of the four analytical stages assesses both pillars in parallel, ensuring neither overshadows the other. The analysis now turns to the first stage, a systematic baseline assessment of resilience across the communications ecosystem.

II. Network Resilience Policy Mapping (NRPM): Baseline Capability Inventory

The **Network Resilience Policy Mapping (NRPM)** establishes a baseline assessment of resilience capabilities across the communications ecosystem. It evaluates three policy pillars, **Protect, Diversify, and Govern**, across four dimensions: **Policy Maturity (PM)**, which assesses the existence and comprehensiveness of policy frameworks; **Implementation (Im)**, which evaluates the extent to which policies are translated into practice; **Institutional Support (IS)**, which measures governance capacity, coordination mechanisms, and stakeholder engagement; and **Resilience Capability (RC)**, which assesses the ecosystem's ability to anticipate, withstand, respond to, and recover from disruptions.

Each dimension is scored on a **1 to 3** scale, where **1** represents limited or fragmented capability, **2** represents moderate capability with partial implementation or identifiable gaps, and **3** represents strong, comprehensive, and well-established capability.

The four scores are aggregated to produce a maximum score of **12** for each pillar. Overall scores of **9 to 12** indicate **High** resilience, **6 to 8** indicate **medium** resilience, and **5 or below** indicate **Low** resilience.

Pillar	Policy Area	PM	Im	IS	RC	Score	Rationale
Protect	Submarine cable resilience	2	1	1	1	**5/12**	**Policy frameworks** emerging, but **redundancy** and **repair capacity** remain **insufficient**; **SIDS** highly exposed to **single points of failure**.
	Telecoms network resilience	3	3	3	3	**12/12**	**Comprehensive resilience obligations** and **proven operational performance** during major disruptions, including the **Red Sea cable incidents**.
	Data centre resilience	3	3	2	3	**11/12**	Supported by **mature international standards** and **widespread adoption** of **redundancy** and **continuity practices**.
	Backup power & site resilience	3	2	2	3	**10/12**	**Strong technical standards** exist, though **deployment remains uneven** across operators and regions.
Diversify	Vendor diversification	3	2	2	1	**8/12**	**Policy support** is increasing, but **market concentration** limits **practical diversification**.
	Open RAN	2	1	1	1	**5/12**	**Policy momentum** is growing, yet **commercial deployment** and **ecosystem maturity** remain **limited**.
	Semiconductor resilience	3	1	1	1	**6/12**	**Significant public investment** is underway, but **supply chain diversification** will take years to **materialise**.
	Software supply-chain security	3	2	3	2	**10/12**	**Mature governance frameworks** strengthened following recent **software supply chain incidents**.
	Cloud diversification	2	1	1	1	**5/12**	**High market concentration** persists, with **limited regulatory measures** to encourage **diversification**.
	Internet infrastructure resilience	3	2	2	1	**8/12**	**Key routing security standards** exist, but **adoption** remains **voluntary** and **uneven**.
Govern	Critical infrastructure regulation	3	3	3	3	**12/12**	**Well established regulatory frameworks** with **clear obligations**, **oversight mechanisms**, and **enforcement powers**.
	Business continuity planning	3	3	2	3	**11/12**	**Widely institutionalised** and **regularly tested** through **operational** and **crisis response exercises**.
	Emergency preparedness	3	2	3	2	**10/12**	**Strong national preparedness frameworks** exist, although **international coordination** remains **inconsistent**.
	Information sharing	3	2	3	2	**10/12**	**Established public private coordination mechanisms**, but **effectiveness varies** across **jurisdictions** and **incidents**.
	International coordination	2	1	1	1	**5/12**	**Global cooperation mechanisms** exist, though **implementation** and **enforcement** remain **fragmented**.
	Cybersecurity frameworks	3	3	3	3	**12/12**	**Mature, internationally recognised frameworks** providing **comprehensive guidance** for **resilience** and **risk management**.

■ High / Sufficient / Strong ■ Medium / Partially Sufficient / Moderate ■ Low / Weak / Critical Gap

Protection and Governance emerge as the strongest pillars, with telecommunications network resilience and cybersecurity frameworks achieving maximum scores of **12/12**. The principal weaknesses lie in **Open RAN (5/12), cloud diversification (5/12), and submarine cable resilience (5/12)**. These are not merely low-scoring areas; they represent growing risks as communications networks become increasingly dependent on a small number of global suppliers and critical infrastructure.

Within the **Protect** pillar, telecommunications network resilience (12/12) and data centre resilience (11/12) reflect mature, well-implemented protection policies (TIA, 2021). In contrast, submarine cable resilience (5/12) exposes a critical vulnerability at the network's most exposed edge (ENISA, 2023). The **Diversify** pillar scores consistently lower across vendor diversification, Open RAN, semiconductor resilience, and cloud diversification, indicating that reducing supply chain dependence, rather than strengthening physical infrastructure, has become the report's central policy challenge (GSMA, 2023; O-RAN Alliance, 2024).

This reflects an implementation gap rather than a legislative one. While policies recognise the need for diversification, commercially viable alternatives—particularly for Open RAN and cloud services—remain limited. As a result, many countries continue to depend on a small number of suppliers, reducing resilience during major disruptions.

The gap also has a significant equity dimension. Tonga and several Pacific Island states rely on a single submarine cable as their only international connection, with no terrestrial fallback (World Bank, 2023; UNCTAD, 2022). Similarly, many African nations depend on a limited number of undersea cable corridors (African Union Commission, 2022).

Applying the **NRPM** to these contexts produces lower resilience scores, demonstrating that resilience depends not only on policy but also on geography, market structure, and available resources.

Addressing these disparities is essential for effective emergency preparedness. Having identified where resilience gaps exist, the analysis now turns to the **Network Resilience Stress-Test Matrix (NRSTM)** to assess how these frameworks perform during real-world disruptions.

III. Network Resilience Stress-Test Matrix (NRSTM): Performance Under Real Disruptions

Policy documents describe resilience on paper, but the **Network Resilience Stress Test Matrix (NRSTM)** examines how resilience performs when disruption occurs.

It evaluates **six real world disruptions** across four resilience dimensions: **Protection (P)**, which assesses preventive measures; **Continuity (C)**, which measures the ability to maintain essential services during disruption; **Adaptation (A)**, which evaluates the capacity to respond and adjust to evolving conditions; and **Recovery (R)**, which assesses how quickly services can be restored.

Each dimension is scored on a **1 to 4** scale, resulting in a maximum score of **16** for each case study.

A score of **1** indicates **limited capability**, **2** indicates **basic capability with significant gaps**, **3** indicates **strong capability with minor limitations**, and **4** indicates **highly resilient performance** demonstrated through effective preparedness, response, and recovery. Overall scores of **13 to 16** indicate **High** resilience, **9 to 12** indicate **Moderate**, **5 to 8** indicate **Low**, and **4 or below** indicate **Very Low** resilience.

Table 2 — NRSTM Stress-Test Results: Resilience Under Real Disruptions

Stress Event	Type	P	C	A	R	Score	Rating	Key Finding
Red Sea Cable Disruptions (2024)	Infrastructure	3	4	3	4	**14/16**	**Strong**	**Route diversity** and **network redundancy** successfully **limited-service disruption** despite **significant physical infrastructure damage**.
CrowdStrike Global Outage (2024)	Dependency	1	2	3	3	**9/16**	**Moderate**	**A single software failure** triggered **widespread disruption**, exposing **systemic risks** arising from **digital dependencies** and **common mode failures**.
COVID-19 Semiconductor Crisis	Dependency	1	2	2	2	**7/16**	**Moderate**	**Concentrated semiconductor supply chains** created **prolonged shortages**, underscoring the strategic importance of **diversification** and **domestic capacity**.
Tonga Submarine Cable (2022)	Infrastructure	1	0	1	1	**3/16**	**Weak**	**Reliance on a single international cable** resulted in **near total national isolation**, highlighting the critical need for **connectivity redundancy**.
Ukraine Communications Disruptions	Geopolitical	2	2	3	2	**9/16**	**Moderate**	**Network resilience measures** sustained **essential connectivity** under conflict conditions, though **service capacity** and **quality** were significantly degraded.
Storm Melissa, Jamaica	Natural Disaster	2	2	2	2	**8/16**	**Moderate**	**Simultaneous damage** to **communications infrastructure**, **power systems**, and **repair capabilities** revealed the **cascading nature of resilience failures**.

■ High / Sufficient / Strong ■ Medium / Partially Sufficient / Moderate ■ Low / Weak / Critical Gap

The scoring spread, from **14/16** for the **Red Sea disruption** to **3/16** for the **Tonga cable failure**, reflects **not the severity of the events but the availability of alternatives**. The **NRSTM** demonstrates that resilience depends less on the strength of individual assets than on **network architecture**. Where **redundant routes** existed, disruption was contained; where they did not, **entire nations lost connectivity**.

"Resilience is not the absence of failure; it is the presence of alternatives."

The case studies also show that **resilience extends beyond physical infrastructure**. The **CrowdStrike outage** demonstrated that no level of **physical hardening** or **network redundancy** could prevent a failure triggered by a **single software update** deployed across millions of devices. Similarly, the **semiconductor crisis** showed that resilient communications depend on **secure industrial and supply chains**. **Emergency preparedness** must therefore encompass the **broader digital ecosystem**, not just physical infrastructure (United States Government, 2019).

Together, these cases reveal **two key resilience gaps**. While **current policies** are relatively effective against **traditional physical disruptions**, they are less prepared for **dependency-driven risks** across **digital and supply chain ecosystems**. The **Tonga cable failure** reflects the structural vulnerabilities of **island and developing economies**, whereas the **CrowdStrike outage** illustrates how **digital dependencies** can bypass physical defenses entirely.

The evidence suggests that **future resilience** depends not only on **protecting infrastructure** but also on **reducing critical dependencies** before they become **single points of failure**. Having assessed both **policy design** and **operational performance**, the analysis now turns to the next question: **Are today's resilience capabilities sufficient for tomorrow's threats?**

IV. Network Resilience Sufficiency Index (NRSI): Forward Adequacy Assessment

The **Network Resilience Sufficiency Index (NRSI)** asks a forward-looking question: given accelerating technological change, geopolitical uncertainty, and growing digital dependencies, are today's capabilities sufficient for tomorrow's threats? It assesses each area across four dimensions: **Capability Maturity (CM)**, which measures the current level of resilience; **Future Risk Exposure (FRE)**, which evaluates vulnerability to emerging threats; **Strategic Importance (SI)**, which assesses the criticality of the capability to communications resilience; and **Sufficiency (S)**, which indicates whether current capabilities are adequate for future challenges. Each dimension is scored on a **1 to 3** scale, where **1** indicates low preparedness, **2** indicates partial preparedness, and **3** indicates strong preparedness, resulting in a maximum score of **12**.

Table 3 — NRSI Forward Sufficiency Assessment: Capabilities Against Future Risks

Capability Area	CM	FRE	SI	S	Score	Rating	Forward Assessment
Cybersecurity Resilience	3	3	3	2	**11/12**	**Sufficient**	**Rapidly evolving AI enabled threats** will require **continuous capability enhancement** and **adaptive governance**.
Telecoms Network Resilience	3	2	3	2	**10/12**	**Sufficient**	**Strong resilience foundations** exist, but **implementation gaps** persist in **developing countries** and **SIDS**.
Software Supply-Chain Security	2	3	3	2	**10/12**	**Sufficient**	**Recent reforms** have strengthened resilience, though **adoption** and **assurance practices** remain **uneven** across ecosystems.
Semiconductor Resilience	1	3	3	1	**8/12**	**Partially Sufficient**	**Diversification efforts** are underway, but **supply chains** remain **concentrated** and **strategic autonomy** remains a long-term objective.
Submarine Cable Resilience	1	3	3	1	**8/12**	**Partially Sufficient**	**Limited route diversity** and **repair capacity** continue to pose **significant systemic risks**, particularly for **SIDS**.
Cloud Diversification	1	3	3	1	**8/12**	**Partially Sufficient**	**Growing hyperscale concentration** may create **systemic dependencies** without stronger **diversification incentives**.
International Coordination	1	3	3	1	**8/12**	**Partially Sufficient**	**Cross border infrastructure risks** increasingly require **institutionalized mechanisms** for **international cooperation** and **crisis response**.
Open RAN & Vendor Diversification	1	2	3	1	**7/12**	**Partially Sufficient**	**Broader deployment** will depend on **ecosystem maturity**, **interoperability**, and **commercial viability** at scale.

■ High / Sufficient / Strong ■ Medium / Partially Sufficient / Moderate ■ Low / Weak / Critical Gap

The **NRSI** reveals a clear pattern. The four areas rated **Partially Sufficient**, **cloud diversification**, **submarine cable resilience**, **semiconductor resilience**, and **international coordination**, also face the **highest future risk** and carry the **greatest strategic importance**. This suggests that dependency is increasing fastest where resilience capabilities remain least developed.

These are not isolated weaknesses but **interconnected vulnerabilities**. A disruption caused by a **semiconductor shortage**, cascading through **cloud services** and affecting countries with **limited connectivity alternatives**, is no longer a hypothetical scenario but a plausible emergency preparedness challenge.

The picture is even more concerning for **SIDS** and **developing economies**, where limited infrastructure and connectivity options further reduce resilience. Capabilities that appear sufficient in advanced economies may prove inadequate in the most exposed regions, highlighting the need for more equitable resilience strategies.

Together, the NRPM, NRSTM, and NRSI deliver a consistent message. Future resilience will depend not only on strengthening infrastructure, but on reducing critical dependencies before they become systemic failures. With the key resilience gaps identified, the analysis now turns to their underlying causes before presenting the **Network Resilience Action Framework**.

V. Why the Gaps Persist: Structural Trade-Offs

Three findings remain consistent across all assessment stages: **protection is strong**, **supply chain diversification is weak**, and the consequences fall hardest on those least able to respond. The question is no longer why these gaps exist, but why do they persist despite sustained policy attention.

The first explanation is the **efficiency of resilience trade off**. Concentration across **cloud services**, **vendor ecosystems**, and **semiconductor manufacturing** reflects economic realities rather than policy neglect. Hyperscale cloud platforms and advanced semiconductor facilities deliver significant cost, innovation, and performance benefits, but also create strategic dependencies. The policy challenge is therefore not to eliminate concentration, but to manage its risks through **interoperability**, **portability**, and **strategic redundancy** that strengthen resilience without undermining efficiency (European Commission, 2022a).

The second explanation is **structural underinvestment**. Measures such as **backup cables**, **reserve network capacity**, and **semiconductor stockpiles** require substantial investment but generate limited short-term returns. As a result, private operators have weak commercial incentives to invest, making **regulatory requirements**, **public private partnerships**, and **shared funding mechanisms** essential to strengthen resilience (OECD, 2023).

The third explanation is the **international coordination gap**. While communications networks, cloud platforms, submarine cables, and semiconductor supply chains operate globally, resilience policies remain largely national. This mismatch leaves the most interconnected infrastructure governed by fragmented coordination mechanisms (International Telecommunication Union, 2023; MANRS, 2024). The low scores for **international coordination** in both the **NRPM** and **NRSI** reinforce this finding. The consequences are greatest for **developing economies** and **SIDS**, which often lack the market scale and resources to offset weaknesses in global governance.

Together, these findings show that resilience gaps are driven less by a lack of awareness than by structural economic and governance constraints. Addressing them will require coordinated action that balances efficiency, investment, and international cooperation. The analysis now turns to the **Network Resilience Action Framework**, translating these findings into a sequenced set of policy priorities.

VI. Network Resilience Action Framework (NRAF): From Diagnosis to Action

The **Network Resilience Action Framework (NRAF)** translates findings from the three preceding assessment stages into a sequenced set of policy priorities across three tiers. **Immediate** priorities address urgent resilience gaps where near term action is feasible. **Strategic** priorities focus on long term investments requiring sustained industrial and institutional development. **Sustain** priorities preserve and strengthen existing resilience capabilities.

Table 4 — NRAF Priority Action Framework: Sequenced Policy Interventions

Priority Area	NRPM	NRSI	Policy Recommendation	Action Tier
Submarine Cable Resilience	Low	**Partially Suff.**	Mandate **minimum redundancy**; **international funding** for SIDS; **diversify** cable landing stations	**Immediate (P1)**
Cloud & Hyperscaler Concentration	Low	**Partially Suff.**	Cloud **portability mandates**; multi-cloud obligations for critical infrastructure; market-share **resilience thresholds**	**Immediate (P2)**
International Coordination	Low	**Partially Suff.**	Binding **global resilience standards**; joint stress-testing; inclusive incident response frameworks	**Immediate (P3)**
Semiconductor Resilience	Med	**Partially Suff.**	**Accelerate** fabrication diversification; strategic reserve frameworks; allied-nation supply cooperation	**Strategic (P4)**
Vendor Diversification & Open RAN	Low–Med	**Partially Suff.**	**Scale** Open RAN deployments; support interoperability; **incentivise** alternative supplier ecosystem	**Strategic (P5)**
Cybersecurity Resilience	High	**Sufficient**	**Continuous** adaptation for AI-enabled threats; extend to emerging attack surfaces	**Sustain (P6)**
Telecoms Network Resilience	High	**Sufficient**	Maintain strengths; **extend modernisation to underserved regions and SIDS**	**Sustain (P7)**

■ Immediate ■ Strategic ■ Sustain

The **NRAF** reflects a key insight: resilience gaps differ in both **urgency** and **time horizon**. **Submarine cable resilience**, **cloud concentration**, and **international coordination** require immediate action because risks are already evident and policy levers exist. **Semiconductor resilience**, **vendor diversification**, and **Open RAN** require sustained investment to reduce future dependencies. Meanwhile, **cybersecurity** and **telecommunications network resilience** must be continuously strengthened to preserve existing capabilities.

Three priorities require immediate action. First, strengthen **submarine cable resilience** by introducing minimum redundancy requirements, expanding cable route diversity, and providing international funding support for **SIDS** and **developing economies** to reduce single points of failure (International Cable Protection Committee, 2022; European Commission, 2024a; European Commission, 2024c). Second, improve **cloud resilience** through **portability**, **interoperability**, and **multi cloud** requirements for critical public services, alongside enhanced resilience obligations for dominant providers (European Commission, 2024b). Third, strengthen **international coordination** by establishing binding resilience standards, regular cross border stress testing, and coordinated incident response mechanisms through **ITU** and **OECD** frameworks (International Telecommunication Union, 2023; OECD, 2022; European Commission, 2022b; European Commission, 2022c).

Strategic priorities focus on building long term industrial and institutional capacity. This includes accelerating **Open RAN** deployment, diversifying **semiconductor manufacturing**, and strengthening international **supply chain cooperation** (GSMA, 2023; O RAN Alliance, 2024; United States Congress, 2022). Because these capabilities take years to mature, early investment is essential. **The longer action is delayed, the more difficult and costly future resilience becomes** (European Commission, 2022a; Semiconductor Industry Association, 2024).

Finally, **cybersecurity** and **telecommunications network resilience** represent hard won strengths that must continue to evolve. As **AI enabled threats** to accelerate, resilience will depend on continuous adaptation rather than one time investment (NIST, 2024). Progress demonstrated during events such as the **Red Sea cable disruptions** must be extended to **SIDS** and underserved regions, where vulnerabilities remain greatest (UK Government, 2022).

The NRAF demonstrates that effective emergency preparedness is not achieved through a single policy intervention, but through a balanced strategy that protects critical infrastructure, reduces strategic dependencies, and strengthens international cooperation. With the policy priorities established, the conclusion draws together the report's key findings and their implications for future communications resilience.

VII. Conclusion: What Must Change

This **essay** set out to answer a fundamental question: **are existing resilience frameworks sufficient to safeguard ICT systems and infrastructure against future disruptions?** Using the **author's original four-stage analytical framework**—Network Resilience Policy Mapping (NRPM), Network Resilience Stress-Test Matrix (NRSTM), Network Resilience Sufficiency Index (NRSI), and Network Resilience Action Framework (NRAF)—the assessment reaches a clear conclusion: **current resilience frameworks are only partially sufficient.**

The analysis finds that **physical telecommunications infrastructure is broadly resilient**, but the wider digital ecosystem remains vulnerable. **Cloud concentration, semiconductor supply chains, software dependencies, submarine cables, and fragmented international coordination** have emerged as the most significant systemic risks. These interconnected dependencies can amplify disruptions, with developing economies and **Small Island Developing States (SIDS)** facing the greatest exposure.

The findings also show that the resilience challenge is shifting from **infrastructure protection to strategic dependency management**. As AI-enabled threats, geopolitical tensions, and digital interdependencies continue to evolve, resilience must be treated as a **continuous strategic capability**, not a one-time policy objective.

Accordingly, this **essay** identifies **three priorities** for effective emergency preparedness: **strengthening critical infrastructure resilience, accelerating supply chain diversification, and deepening international cooperation.** Ultimately, resilience will be determined not by preventing every disruption, but by ensuring that **no single point of failure can compromise essential communications**, enabling a more secure, adaptive, and future-ready digital ecosystem.

Beyond the Competition

Looking Ahead

"If I had the opportunity to work on this beyond this competition, where would this framework evolve?"

Long-Term Vision

- To evolve these four frameworks into an **open**, **evidence-based policy toolkit** that governments, regulators, and international organizations can use to **assess, benchmark, and strengthen communications resilience across diverse national contexts**

Framework Evolution

- The framework is designed to follow a simple but enduring **logic: map, stress-test, assess, and act.** While **this progression will remain its defining principle**, future iterations should strengthen each stage through more robust scoring, greater consideration of interdependencies, validation across different national contexts, and continuous refinement informed by real-world disruptions and emerging technologies**.**

Bibliography

African Union Commission (2022). Digital Transformation Strategy for Africa 2020–2030. Addis Ababa: AU Commission.
Carnegie Endowment for International Peace (2024). Securing Europe's Subsea Data Cables. Washington DC: Carnegie Endowment for International Peace.
ENISA (2023). Dive into the Deep Sea: A View of the Subsea Cable Ecosystem. Athens: European Union Agency for Cybersecurity.
European Commission (2022a). European Chips Act: Regulation (EU) 2023/1781. Brussels: European Commission.
European Commission (2022b). NIS2 Directive: Directive (EU) 2022/2555. Brussels: European Commission.
European Commission (2022c). CER Directive: Directive (EU) 2022/2557. Brussels: European Commission.
European Commission (2024a). EU Action Plan on Cable Security. Brussels: European Commission.
European Commission (2024b). EU Data Act: Regulation (EU) 2023/2854. Brussels: European Commission.
European Commission (2024c). Commission Recommendation (EU) 2024/779 on Secure and Resilient Submarine Cable Infrastructures. Brussels: European Commission.
GSMA (2023). Driving Supply Chain Resiliency for Open RAN Development. London: GSMA.
International Cable Protection Committee (2022). ICPC Recommendations and Reports on Submarine Cable Faults and Protection. Lymington: ICPC.
International Telecommunication Union (2023). Global Cybersecurity Index 2024. Geneva: ITU.
ISO (2019). ISO 22301:2019 — Security and Resilience — Business Continuity Management Systems. Geneva: ISO.
MANRS (2024). Mutually Agreed Norms for Routing Security. Available at: https://www.manrs.org
NIST (2024). Cybersecurity Framework 2.0. Gaithersburg: NIST.
NIST (2022). Secure Software Development Framework (SSDF), SP 800-218. Gaithersburg: NIST.
OECD (2022). OECD Policy Framework on Digital Security: Cybersecurity for Prosperity. Paris: OECD.
OECD (2023). Enhancing the Security of Communication Infrastructure. Paris: OECD.
O-RAN Alliance (2024). O-RAN Technical Specifications and White Papers. Available at: https://www.o-ran.org
Semiconductor Industry Association (2024). 2024 State of the U.S. Semiconductor Industry. Washington DC: SIA.
TIA (2021). TIA-942-B: Telecommunications Infrastructure Standard for Data Centers. Arlington: TIA.
UK Government (2022). Telecommunications Diversification Strategy. London: DCMS.
UNCTAD (2022). Technology and Innovation Report 2022. Geneva: UNCTAD.
UNDRR (2015). Sendai Framework for Disaster Risk Reduction 2015–2030. Geneva: United Nations Office for Disaster Risk Reduction.
United Nations (1998). Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations. Geneva: United Nations.
United States Congress (2022). CHIPS and Science Act of 2022, Public Law 117-167. Washington DC: U.S. Government Publishing Office.
United States Government (2019). National Response Framework, 4th edition. Washington DC: FEMA.
World Bank (2023). Digital Progress and Trends Report 2023. Washington DC: World Bank.
World Economic Forum (2024). Global Risks Report 2024. Geneva: World Economic Forum.

Use of Artificial Intelligence

Artificial intelligence tools — specifically Claude (Anthropic) — were used in a supporting capacity during the drafting and editing process, including structural editing and prose refinement to improve clarity and flow, formatting and presentation of tables and framework elements, and checking consistency of terminology across sections. **All analytical judgements, scoring decisions, policy arguments, and substantive conclusions are the author's own. The four-stage analytical framework (NRPM, NRSTM, NRSI, NRAF) was developed independently by the author. AI tools did not generate the core**