Leapfrogging Institutions: A Digital Development Model for SIDS

True digital transformation requires skipping legacy bureaucracy in favour of agile, digitally native governance.

Tech Leapfrogging

- Skipping landlines for mobile networks
- Hardware-centric model
- Purchasing external technology without local foundational governance

The DPI Imperative

Digital Public Infrastructure as the sovereignty, resilience, and sustainable development.

Institutional Leapfrogging

- Skipping legacy bureaucracy
- Digitally native governance
- Building capacity and frameworks for responsible State behaviour

The DPI Imperative demands a bespoke model for Pacific Small States

Importing legacy regulatory frameworks stifles innovation; SIDS require lean, foundational infrastructure designed for scale and agility.

The EU Model (Legacy)

Approach: Heavy Regulation

Rule-making precedes infrastructure deployment.

Infrastructure: Legacy Systems

Burdened by decades of analogue institutional debt.

Governance: Fragmented Sovereignty

Complex, multi-layered jurisdictional overlap.

Pacific Small States (Greenfield)

Approach: Agile Policy

Dynamic frameworks adapting to rapid technological shifts.

Infrastructure: Greenfield DPI

Building natively digital public infrastructure from the ground up.

Governance: Pooled Regional Sovereignty

Leveraging regional bodies and shared resources to amplify diplomatic and technical weight.

A layered architecture for oceanic connectivity

Aligning international law and UN GGE norms into a cohesive stack for digital sovereignty.

SMART (Innovation)

The Future Layer

- Harnessing AI, quantum computing, and digital broadcasting.
- Fostering local IT talent and bridging the digital divide.
- Ensuring states compete globally on an equal footing.

SECURE (Trust)

The Logical & Social Layer

- Implementing UN GGE/OEWG norms of responsible State behaviour.
- Establishing incident management mechanisms and protecting critical infrastructure.
- Safeguarding human rights online.

RESILIENT (Continuity & Sovereignty)

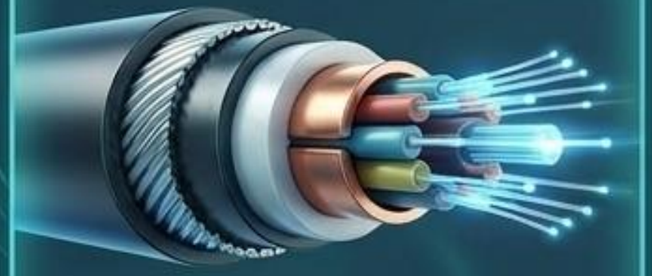
The Physical Layer

- Protection of submarine communications cables (carrying over 95% of transoceanic internet traffic).
- Rooted in UNCLOS Articles 113-115, ensuring continuity against human-activity faults and physical threats.

IGF Internet Governance Forum

The Industrial Policy Toolkit for SIDS

Translating international legal obligations and capacity-building mandates into strategic regional policy.



1. Physical Protection of Submarine Cables

- Enacting domestic criminal legislation to penalise culpable negligence or wilful injury to cables (UNCLOS).
- Establishing monitoring systems to mitigate the 80% of cable faults caused by human activity (e.g., fishing, anchoring).

2. Regional Resource Pooling

- Establishing community information networks and shared mechanisms for crisis management.
- Partnering with regional and sub-regional organisations to implement localised capacity-building initiatives.
- Sharing critical threat intelligence across jurisdictions.

3. Global Capacity Building

- Leveraging the UN OEWG Dedicated Thematic Group.
- Developing human resources and accessing industry transparency centres.
- Utilising international arrangements for the mutual recognition of certified ICT products.

IGF Internet Governance Forum

Horizon 2030: Realising Digital Development Goals

Capacity-building is foundational to accelerating digital transformation and securing the 2030 Agenda.

Milestone 1:
Resilient Physical Backbone

- Zero critical submarine cable outages. Domestic legislation actively protects the sovereign physical layer.

Milestone 2:
Institutional Agility

- Full integration of UN norms of responsible State behaviour.
- DPI operates securely, fostering an open and safe ICT environment.

Milestone 3:
Sustainable Digital Equality

- The digital divide is bridged.
- Citizens' fundamental rights are protected online, and SIDS compete globally on an equal footing.

"Capacity-building is foundational to developing the resources, skills, policies and institutions necessary to increase the resilience and ICT security of States..."

— UN OEWG Final Report

IGF Internet Governance Forum