AI-slands

Intelligent Islands or Dependent Islands?

AI Infrastructure, Energy and Digital Sovereignty

Andrew Jennings
Professor in Island Studies
Institute for Northern Studies
University of the Highlands and Islands

AI-slands Working Paper No. 6 | 2026

AI-slands research initiative: ai.insularworlds.co.uk

Suggested citation: Jennings, A. (2026) *Intelligent Islands or Dependent Islands? AI Infrastructure, Energy and Digital Sovereignty*. AI-slands Working Paper No. 6. Institute for Northern Studies, University of the Highlands and Islands.

Abstract

Artificial intelligence is often presented as software that arrives through a browser or application. For islands, however, AI is a physical and institutional system. It depends on international cables and satellites, data centres and cloud providers, electricity and cooling, locally relevant data, skilled people, contracts and rules. Each layer can widen opportunity, but each can also create a dependency whose effects are sharper where networks are thin, energy systems are bounded and public purchasing power is small.

This working paper examines how islands can pursue AI capability without confusing digital sovereignty with technological self-sufficiency. Tonga's 2022 cable damage demonstrates the consequences of limited routes. The Faroese-owned SHEFA network shows how island institutions can own infrastructure while remaining embedded in international systems. Ireland's data-centre electricity demand and Singapore's capacity planning show that compute competes for scarce power and requires public allocation choices. Barbados has proposed a national data centre as public digital infrastructure, while Mauritius has operated a central Government Online Centre since 2005. Māori data-sovereignty practice in Aotearoa New Zealand shows that control also concerns collective authority over data, models and permitted uses.

The paper proposes a five-layer Island AI Infrastructure Stack and an Island Digital Sovereignty Test. Its central argument is that sovereignty should be understood as governed interdependence: the practical capacity to choose, negotiate, inspect, switch, recover and retain public value. Building a data centre does not by itself create sovereignty, and using an overseas cloud does not by itself remove it. The decisive questions are who controls essential decisions, what happens when a provider or connection fails, which local resources bear the cost, and whether island communities can shape or refuse the resulting system.

Keywords: artificial intelligence; islands; digital sovereignty; data centres; cloud computing; energy; subsea cables; data governance; resilience

Evidence note

The references are limited to sources whose existence, bibliographical details and relevance to the cited claim were checked against journal, publisher, government, intergovernmental or institutional records. Complete texts or relevant pages were inspected wherever accessible. DOI, repository and stable institutional links are supplied. Statistics are tied to their stated period and unit. Official statements about planned facilities are treated as proposals rather than completed infrastructure, and operator descriptions are attributed rather than presented as independent evaluations. Much published environmental evidence covers data centres or computing in general rather than an identifiable AI-only share; the paper preserves that limitation.

1. AI has an island geography

An AI service can feel placeless. A user types into a screen and receives an answer without seeing the cable landing station, power plant, server hall, cooling system, dataset or contract that made the exchange possible. This appearance is misleading. AI rests on a chain of material assets and institutional decisions, and geography affects every link.

The World Bank's 2025 account of AI foundations identifies connectivity, compute, context and competency as four requirements for participation. It also observes that high-income countries dominate AI innovation and compute infrastructure, while the supply of compute is concentrated among a small number of firms (World Bank, 2025). For islands, those foundations are shaped by sea crossings, small electricity markets, limited specialist capacity and long supply chains. Context

must also include island languages, public records, environmental knowledge and the authority to determine how such material is used.

The energy implications are substantial. The International Energy Agency estimates that data centres consumed about 415 terawatt-hours of electricity worldwide in 2024 and projects consumption of about 945 terawatt-hours in 2030, with AI the main driver of the increase (IEA, 2025, pp. 13, 62-63). These are scenarios rather than island forecasts. They nevertheless establish that AI policy is also electricity policy. A new computing load must connect to a grid at a particular place and time. It may compete with housing, electrified transport, industry and public services for network capacity and generation.

Environmental accounting must extend beyond operational electricity. The OECD distinguishes the direct effects of producing, transporting, operating and disposing of computing resources from the indirect effects of AI applications. It finds weak and non-standardised disclosure, particularly for water consumption and full lifecycle effects (OECD, 2022, pp. 18-21, 34-36). UNCTAD similarly places digital infrastructure within a lifecycle of mineral extraction, equipment production, energy and water use, and electronic waste (UNCTAD, 2024). Island governments therefore need evidence about the whole infrastructure proposal, not a marketing claim that renewable electricity makes a data centre green.

This material perspective changes the policy question. The issue is not whether an island should be connected or disconnected from global AI. Complete separation would deny access to capabilities that no small jurisdiction can efficiently reproduce. The issue is which dependencies are acceptable, visible and governable, and which leave an island unable to continue an essential service or alter an unfavourable arrangement.

2. From autonomy to governed interdependence

Digital sovereignty is used to describe different political projects. Couture and Toupin show that the term has referred to independence, control and autonomy over infrastructure, technologies and data, but that its subject may be a state, an Indigenous people, a social movement or an individual (Couture and Toupin, 2019). Pohle and Thiel likewise caution that digital sovereignty is a contested political practice rather than a settled legal condition. They connect it to state authority, economic capacity, infrastructural security and individual self-determination (Pohle and Thiel, 2020).

This plurality is especially useful for islands. A state may possess legislative authority while relying on foreign cables, cloud regions, software licences and technical staff. A non-sovereign island may have little formal power over telecommunications regulation but strong community institutions, public ownership or procurement influence. An Indigenous nation may exercise collective authority over data without controlling the national grid. Sovereignty cannot be measured by constitutional status alone.

Nor should it be equated with owning every asset. A locally owned server room can depend on imported equipment, proprietary software and a single cable. An overseas cloud service may offer better security, redundancy and cost than a small local installation. The location of a server matters for latency, law, resilience and local economic value, but data residency does not answer who can access the data, change the terms, audit the model or move the workload.

For this paper, island digital sovereignty means the practical and legitimate capacity of island institutions and communities to make consequential choices about digital systems. Six capabilities make that idea operational:

1. **Choice** among technically and legally credible options.

2. **Negotiation** of price, service, jurisdiction and public-interest conditions.

3. **Inspection** of performance, environmental cost, data use and security.

4. **Switching** through portable data, interoperable systems and workable exit terms.

5. **Recovery** when a cable, grid, facility or provider fails.

6. **Value retention** through local skills, ownership, public revenue and community benefit.

These capabilities amount to governed interdependence. Dependence is not eliminated; it is made legible, bounded and contestable. The standard is demanding but more realistic than digital autarky.

3. The Island AI Infrastructure Stack

AI readiness is often reduced to broadband coverage or the presence of a data centre. A layered model exposes where power and risk sit.

Layer	Island question	Typical failure	Sovereignty capability
International connectivity	How many independent routes connect the island, and who owns them?	Cable break, landing-station failure, unaffordable capacity	Route diversity, repair arrangements, satellite or cable backup
Compute and cloud	Where can workloads run, and can they move?	Provider outage, lock-in, loss of service, foreign legal exposure	Portable architecture, multiple suppliers, local or regional fallback
Electricity and cooling	What power, grid and water resources will computing require?	Grid congestion, price pressure, diesel backup, water conflict	Capacity allocation, disclosure, efficiency and environmental limits
Data and models	Who governs training data, public records and model behaviour?	Extraction, cultural harm, inaccessible proprietary systems	Consent, licensing, audit, local adaptation and refusal rights
Institutions and skills	Who can purchase, operate, challenge and repair the system?	Vendor dependence, weak oversight, loss of organisational knowledge	Skilled teams, pooled expertise, transparent contracts and public scrutiny

The layers are interdependent. A locally adapted language model hosted abroad may preserve cultural control over data yet remain vulnerable to pricing or connectivity changes. A national data centre may improve public-sector continuity but consume scarce electricity and still depend on a foreign software stack. A second cable may add resilience but offer little benefit if every public service uses one cloud identity system. Policy should test the chain rather than count isolated assets.

The stack also reveals distribution within archipelagos. A national average can conceal a principal island with fibre, grid capacity and technical staff alongside outer islands using slower or more fragile connections. Redundancy at the national landing point does not guarantee redundant links to every inhabited island. Infrastructure assessment should therefore identify the geography of failure: which communities lose service first, which receive backup and how long restoration takes.

4. Cables and the politics of connection

Submarine cables carry the great majority of international digital traffic, yet their distribution is uneven. Franken and colleagues model state vulnerability to cable failure and show that connectivity resilience varies with the number and configuration of links; countries with fewer alternatives face greater exposure (Franken et al., 2022). Watson's account of Pacific Island communications records the limited cable connections of several states and uses the 2022 Tonga eruption to show the consequences of physical disruption (Watson, 2022).

4.1 Tonga and a visible point of failure

The eruption and tsunami of 15 January 2022 damaged Tonga's international cable from Fiji and its domestic cable system. The World Bank's rapid damage assessment valued the international cable at T$64.9 million, or US$28.2 million, and estimated cable-related damage and works at approximately T$7.8 million, or US$3.4 million (World Bank and Government of Tonga, 2022, pp. 16-17). The incident made a normally hidden dependency publicly visible.

The lesson is not merely that Tonga needed more bandwidth. Essential communications depended on physical routes exposed to the same broad hazard environment. A resilience plan must therefore consider geographic separation, repair contracts, access to specialist vessels, spare equipment, emergency satellite capacity, domestic inter-island links and priority access for health, government and relief organisations.

AI increases the importance of this planning. Cloud-hosted decision support, translation, records systems and forecasting tools may improve services in ordinary conditions. If they cannot operate during a communications failure, they may add a new dependency precisely when local institutions need them most. Procurement should specify a degraded mode: what the system can do locally, which data remain accessible and how staff continue safely without model access.

4.2 The SHEFA network and ownership within a wider system

The North Atlantic supplies a contrasting example. Shefa states that it owns the SHEFA-2 fibre-optic cable linking the Faroe Islands, Shetland and Orkney to Scotland, and that it owns CANTAT-3, which links Iceland and the Faroes towards Denmark and Germany. It also reports access to capacity on FARICE and DANICE (Shefa, 2026a). Its network offers backup routes from the island groups towards the United Kingdom and Denmark (Shefa, 2026b).

This operator account does not establish that every community or internet provider has identical resilience. It does demonstrate a significant form of island agency: an island-based organisation owns international infrastructure and assembles capacity across several routes. Ownership brings knowledge, bargaining position and the ability to plan around island demand. Yet the network remains international, crosses several jurisdictions and depends on mainland landing points. Sovereignty here is relational rather than isolated.

Tonga and SHEFA suggest four questions for cable policy. Are routes physically diverse? Does the island have enforceable restoration priorities? Can traffic be moved through another provider without extensive reconfiguration? Do public authorities know which services share a common point of failure? A cable map alone cannot answer them.

5. Compute competes for island resources

Data centres translate digital ambitions into land, substations, generators, cooling equipment and continuing demand. A 100-megawatt facility can use as much electricity as about 100,000 households, although actual comparisons depend on local consumption patterns and facility load (IEA, 2025, p. 37). The siting decision is therefore distributive. It determines who gains access to constrained infrastructure, who pays for expansion and what other uses are delayed.

5.1 Ireland and the scale of cumulative demand

Ireland provides the clearest official island-state measure. The Central Statistics Office reports that data centres consumed 22 per cent of metered electricity in 2024, up from 5 per cent in 2015. Their consumption reached 6,969 gigawatt-hours in 2024, compared with 18 per cent for urban dwellings and 10 per cent for rural dwellings (Central Statistics Office, 2025). These figures cover data centres as a category, not an AI-only share.

The case demonstrates why each facility cannot be assessed as an isolated investment. Individual projects accumulate within one national grid and influence network planning, generation requirements and climate policy. Employment and tax benefits must be evaluated against infrastructure costs and opportunity costs. Renewable procurement does not remove the need to ask whether new demand requires additional clean generation or displaces other electrification.

Ireland is not a small island developing state, and its grid, economy and European market access distinguish it from many islands. Its relevance lies in the visibility of the trade-off. Publishing a dedicated statistical series allows public discussion to begin from measured consumption rather than estimates supplied by developers. Other island jurisdictions should require comparable disclosure before pursuing compute-intensive development.

5.2 Singapore and planned capacity allocation

Singapore illustrates active management rather than unrestricted growth. Its 2024 Green Data Centre Roadmap aims to provide at least 300 megawatts of additional data-centre capacity in the near term, with further capacity tied to green-energy deployment. The policy combines computing expansion with energy-efficiency measures and access to low-carbon power (Infocomm Media Development Authority, 2024).

Singapore's metropolitan scale, wealth and administrative capacity make it an imperfect comparator for dispersed archipelagos. Even so, the roadmap establishes an important principle: data-centre capacity is something government can allocate and condition. It is not simply a private demand to which the grid must respond. A similar approach on smaller islands would begin with a public capacity envelope covering electricity, network reinforcement, water, land and emergency generation.

The contrast between Ireland and Singapore also cautions against single indicators. Power-usage effectiveness measures how efficiently a facility uses electricity once supplied; it does not show whether the electricity is additional, whether water use is acceptable, whether heat can be reused, or whether the facility serves a public purpose. OECD analysis calls for broader lifecycle measurement and notes the lack of standardised, validated environmental data (OECD, 2022, pp. 34-36). Island authorities should make disclosure a planning condition rather than wait for voluntary reports.

6. Public data centres and the build or buy decision

Governments face a strategic choice between domestic facilities, regional infrastructure and international cloud services. The World Bank describes the decision as whether to build national compute capacity or secure affordable access to international cloud infrastructure (World Bank, 2025). In practice, most islands will use a mixture.

6.1 Barbados and infrastructure as a public proposal

Barbados's 2024 Budget Address announced that the government would establish a National Data Centre to support online government services, health-sector digitalisation and a wider technology industry. The address described implementation over two to three years (Government of Barbados, 2024). The source records a policy commitment, not a completed facility or verified benefit.

The proposal is important because it connects computing infrastructure to public functions and national development rather than presenting a data centre solely as real-estate investment. It also creates questions that should be answered before construction: which workloads require domestic hosting; what cable and power redundancy will support the site; what data classification governs placement; which foreign hardware and software remain indispensable; and whether a regional disaster-recovery arrangement would offer better resilience than a second domestic room.

6.2 Mauritius and an operating government facility

Mauritius offers an operational comparison. The Ministry of Information Technology, Communication and Innovation describes the Government Online Centre as a central data centre serving public institutions and operating continuously. The centre has provided shared hosting and network services for government since May 2005 (Government of Mauritius, 2026). This is evidence of institutional continuity, although the government description is not an independent security or performance audit.

The case shows that public infrastructure is also organisational infrastructure. A shared centre can retain staff knowledge, standardise services and give the state a stronger position when purchasing technology. It can also become a concentrated point of failure or preserve outdated systems if governance and investment do not keep pace. The sovereign value lies in capability and accountable service management, not the building itself.

For both Barbados and Mauritius, a hybrid architecture is likely to be more credible than an absolute rule of local hosting. Highly sensitive registers, emergency functions and services requiring offline continuity may warrant domestic or regional control. Elastic research workloads may be cheaper in global cloud regions. Small AI models can run on local servers or edge devices. The correct mix depends on data sensitivity, latency, energy cost, outage tolerance, portability and the ability to operate the system.

7. Cloud dependence and the right to exit

Cloud services allow islands to access computing without financing hyperscale facilities. They offer rapid deployment, specialist security and capacity that can expand or contract. Those advantages can become structural dependence when an organisation cannot move its data, identity system, software or trained staff to another provider.

The United Kingdom's Competition and Markets Authority completed a market investigation into cloud infrastructure services in July 2025 and recommended consideration of strategic-market-status investigations into Microsoft and Amazon Web Services, the two largest providers (CMA, 2025). Ofcom's preceding study had treated cloud services as essential to the delivery of digital services (Ofcom, 2023). These findings concern the UK market, not every island. They nevertheless matter because many island public bodies purchase from the same firms and may possess less negotiating leverage than large national customers.

An island cloud strategy should therefore begin with exit, not only entry. Contracts should specify usable export formats, data-transfer costs, identity portability, transition assistance, deletion evidence, audit rights and continuity after termination. Architecture should avoid unnecessary dependence on proprietary functions when a standard alternative meets the need. Critical systems should be tested against provider outage and loss of international connectivity.

Multi-cloud procurement is not automatically a solution. Running the same system across providers can increase complexity, cost and skill requirements. A smaller jurisdiction may gain more from shared regional expertise, portable backups and a tested recovery environment than from duplicating every live workload. The objective is a credible alternative, not the appearance of supplier diversity.

8. Data sovereignty completes the infrastructure question

Physical control does not settle authority over data. A government may host records locally while denying communities meaningful say over collection, linkage and reuse. Conversely, a community may govern data held on external infrastructure through enforceable licences, access rules and institutional practice.

Indigenous data sovereignty makes this distinction explicit. Kukutai and Taylor describe Indigenous data sovereignty as the right of Indigenous peoples to govern data about their peoples, lands and resources (Kukutai and Taylor, 2016). Te Mana Raraunga applies this principle in Aotearoa New Zealand, asserting Māori rights and interests in data and supporting Māori governance of repositories and infrastructure (Te Mana Raraunga, 2018).

Te Hiku Media translates these principles into AI practice. Its Māori-led language-technology work includes speech recognition, speech synthesis and pronunciation tools, while its Kaitiakitanga Licence sets conditions intended to keep labelled Māori language data under Māori guardianship and for Māori benefit (ITU, 2022). The case does not depend on owning every server or chip. Its sovereign element is the community institution's authority to determine legitimate use and negotiate access.

This matters across islands because cultural and environmental datasets are often collectively produced. Oral histories, place names, biodiversity observations, fishing knowledge and language recordings may be legally accessible but culturally restricted. An infrastructure strategy that secures a server while licensing its contents to an external model provider can strengthen state control and weaken community control at the same time.

Data governance should therefore classify authority as well as sensitivity. A public body should ask whose data are involved, which collective rights apply, what secondary training uses are proposed, how benefits return and whether consent can be withdrawn. Models trained or fine-tuned on island data should have documented provenance, permitted uses and responsible custodians. Community refusal is a legitimate infrastructure decision because data supply is part of the AI stack.

9. An Island Digital Sovereignty Test

The following test can be applied to an AI strategy, cloud contract, cable investment, data-centre proposal or individual public system.

Dimension	Core question	Minimum evidence
Purpose	Which island need or public function requires this infrastructure?	Defined users, service need and alternatives appraisal
Connectivity	Which independent routes and recovery arrangements support it?	Route map, common-failure analysis and restoration plan
Resource fit	What electricity, water, land and backup fuel will it use?	Measured demand, lifecycle assessment and capacity allocation
Control	Who can set access, use, security and retention rules?	Governance roles, audit rights and enforceable contract terms
Portability	Can data, models and services move to another environment?	Open formats, tested export, transition cost and exit timetable
Continuity	What remains available during cable, grid or provider failure?	Offline or degraded mode, backup power and recovery exercise

Dimension	Core question	Minimum evidence
Community authority	Do Indigenous or community rights apply to the data or knowledge?	Consent, licensing, benefit sharing and refusal mechanism
Local capability	Who can operate, inspect and challenge the system?	Staffing plan, knowledge transfer and independent expertise
Distribution	Which islands receive service, cost and resilience?	Island-disaggregated coverage and impact evidence
Public value	What durable benefit remains locally?	Ownership, revenue, skills, service outcomes and published review

The test should be completed before procurement and repeated during operation. Evidence should be published except where security requires limited disclosure. A proposal that cannot identify its power demand, exit route or outage procedure is not ready for approval.

The test also prevents symbolic sovereignty. A national label, local server address or government-owned building may be valuable, but none substitutes for portability, community authority or operational competence. Conversely, a carefully governed regional service may offer more real control than a nominally domestic system that only one overseas vendor can maintain.

10. A policy programme for sovereign capability

Ten commitments follow from the comparative evidence.

1. **Publish an infrastructure dependency register.** Record the cables, landing stations, cloud providers, identity systems, power assets and specialist suppliers on which essential AI-enabled services depend.
2. **Require geographically credible redundancy.** Test whether alternative routes share the same landing point, terrestrial link, substation, provider or hazard exposure.
3. **Define a public compute portfolio.** Match local, regional and global computing options to workload sensitivity, scale, latency, energy and continuity requirements.
4. **Plan data-centre capacity as a public resource.** Set transparent limits and conditions for electricity, water, land, backup generation and network reinforcement.
5. **Mandate environmental disclosure.** Require measured electricity, water, emissions and equipment-lifecycle information, while identifying the share attributable to AI where this can be measured.
6. **Procure for portability.** Make open export formats, interface documentation, transition support and deletion assurance standard contract requirements.
7. **Protect community and Indigenous authority.** Establish governance, consent, licensing, attribution, benefit sharing and refusal rights before data enter model development.
8. **Fund operational capability.** Invest in engineers, procurement specialists, cyber-security staff, archivists and community data stewards, including career paths that retain expertise.
9. **Build regional institutions.** Pool procurement, incident response, model evaluation, specialist advice and disaster recovery where individual islands lack scale.
10. **Exercise failure plans.** Simulate cable loss, extended power disruption, cloud outage and vendor exit; publish lessons and correct the resulting gaps.

Regional cooperation is particularly important. Shared capacity can produce bargaining power without requiring political uniformity. Islands might jointly maintain contract clauses, accredited

evaluators, emergency satellite equipment, model-testing facilities or a regional recovery cloud. The arrangement should distribute authority and benefits rather than reproduce a capital-island hierarchy at a larger scale.

Local economic development should remain part of infrastructure policy. Cable ownership, public hosting, energy investment and data stewardship can create skilled work and institutional knowledge. Yet job claims should be separated into construction, continuing operations and indirect activity. A capital-intensive facility with few permanent employees may still be valuable, but its public case must rest on measured services, revenue or resilience rather than inflated employment figures.

11. Conclusion

AI gives islands new tools while deepening their reliance on systems located elsewhere. That tension cannot be resolved by choosing either connection or independence. Islands need international networks, specialised chips, cloud services and shared knowledge. They also need the power to decide how these resources enter public life and what happens when they fail.

The cases reveal different forms of agency. Tonga's cable damage exposes the cost of limited physical routes. The SHEFA network shows island ownership operating through international connectivity. Ireland makes cumulative electricity demand statistically visible. Singapore treats data-centre growth as capacity to be allocated and conditioned. Barbados frames a proposed national data centre as public infrastructure, while Mauritius demonstrates the organisational value of a long-running government centre. Māori data-governance practice shows that sovereign control can reside in collective authority over data and permitted use, even where physical computing is distributed.

No single architecture fits every island. A small local data centre may strengthen continuity or become an expensive point of failure. A global cloud may widen access or create costly lock-in. Renewable energy may reduce operating emissions while leaving water, grid capacity and equipment impacts unresolved. The decision must be made at the level of the full stack.

Governed interdependence provides a practical standard. An island has greater digital sovereignty when it can choose and negotiate, inspect what is happening, move when terms become unacceptable, recover from failure and retain value in local institutions and communities. These capabilities can be measured and improved. They are more consequential than whether a server sits within a coastline.

An intelligent island is therefore not the island with the largest model or newest data centre. It is one that knows where its dependencies lie, sets limits according to public purpose and ecological capacity, and preserves the authority to change course.

References

Central Statistics Office (2025) *Data Centres Metered Electricity Consumption 2024*. Dublin: Central Statistics Office, 10 June. https://www.cso.ie/en/releasesandpublications/ep/p-dcmec/datacentresmeteredelectricityconsumption2024/

Competition and Markets Authority (CMA) (2025) *Cloud Services Market Investigation: Final Decision*. London: CMA, 31 July. https://www.gov.uk/cma-cases/cloud-services-market-investigation

Couture, S. and Toupin, S. (2019) 'What does the notion of sovereignty mean when referring to the digital?', *New Media & Society*, 21(10), pp. 2305-2322. https://doi.org/10.1177/1461444819865984

Franken, J., Reinhold, T., Reichert, L. and Reuter, C. (2022) 'The digital divide in state vulnerability to submarine communications cable failure', *International Journal of Critical Infrastructure Protection*, 38, 100522. https://doi.org/10.1016/j.ijcip.2022.100522

Government of Barbados (2024) *2024 Budget Address*. Bridgetown: Office of the Prime Minister, 18 March. https://pmo.gov.bb/2024/03/18/2024-budget-address/

Government of Mauritius (2026) 'Government Online Centre'. Ministry of Information Technology, Communication and Innovation. https://mitci.govmu.org/mitci/government-online-centre/

Infocomm Media Development Authority (2024) 'Singapore launches Green Data Centre Roadmap to guide sustainable growth of digital infrastructure', 30 May. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/sg-announces-green-data-centre-roadmap

International Energy Agency (IEA) (2025) *Energy and AI*. Paris: IEA. https://www.iea.org/reports/energy-and-ai

International Telecommunication Union (ITU) (2022) 'Accelerating the revitalisation of te reo Māori with AI', AI for Good, 26 July. https://aiforgood.itu.int/event/accelerating-the-revitalisation-of-te-reo-maori-with-ai/

Jennings, A. (2026a) *AI-slands: Towards an Island-Centred Approach to Artificial Intelligence*. AI-slands Working Paper No. 1. Institute for Northern Studies, University of the Highlands and Islands. https://ai.insularworlds.co.uk/working-paper-1.html

Jennings, A. (2026b) *AI and Island Cultures: Preservation, Extraction and the Right to Refuse*. AI-slands Working Paper No. 2. Institute for Northern Studies, University of the Highlands and Islands. https://ai.insularworlds.co.uk/working-paper-2.html

Jennings, A. (2026c) *Small Islands, Big Decisions: AI Governance, Dependency and the Right to Shape the Digital Future*. AI-slands Working Paper No. 3. Institute for Northern Studies, University of the Highlands and Islands. https://ai.insularworlds.co.uk/working-paper-3.html

Jennings, A. (2026d) *Bridging the Water: AI, Distance and the Future of Island Services*. AI-slands Working Paper No. 4. Institute for Northern Studies, University of the Highlands and Islands. https://ai.insularworlds.co.uk/working-paper-4.html

Jennings, A. (2026e) *Can AI Help Islands Keep Their People? Work, Demography and Island Futures*. AI-slands Working Paper No. 5. Institute for Northern Studies, University of the Highlands and Islands. https://ai.insularworlds.co.uk/working-paper-5.html

Kukutai, T. and Taylor, J. (eds) (2016) *Indigenous Data Sovereignty: Toward an Agenda*. Canberra: ANU Press. https://doi.org/10.22459/CAEPR38.11.2016

OECD (2022) *Measuring the Environmental Impacts of Artificial Intelligence Compute and Applications: The AI Footprint*. OECD Digital Economy Papers No. 341. Paris: OECD Publishing. https://doi.org/10.1787/7babf571-en

Ofcom (2023) *Cloud Services Market Study: Final Report*. London: Office of Communications, 5 October. https://www.ofcom.org.uk/internet-based-services/cloud-services/cloud-services-market-study

Pohle, J. and Thiel, T. (2020) 'Digital sovereignty', *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1532

Shefa (2026a) 'The Shefa Network'. https://www.shefa.fo/elbowroom/

Shefa (2026b) 'Connecting Islands'. https://www.shefa.fo/connecting-islands/

Te Mana Raraunga (2018) *Principles of Māori Data Sovereignty*. Māori Data Sovereignty Network. https://www.temanararaunga.maori.nz/principles-of-maori-data-sovereignty

United Nations Conference on Trade and Development (UNCTAD) (2024) *Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future*. Geneva: United Nations. https://unctad.org/publication/digital-economy-report-2024

Watson, A.H.A. (2022) 'The limited communication cables for Pacific Island countries', *Asia-Pacific Journal of Ocean Law and Policy*, 7(1), pp. 151-155. https://doi.org/10.1163/24519391-07010012

World Bank (2025) *Digital Progress and Trends Report 2025: Strengthening AI Foundations*. Washington, DC: World Bank. https://www.worldbank.org/en/publication/dptr2025-ai-foundations/report

World Bank and Government of Tonga (2022) *The January 15, 2022 Hunga Tonga-Hunga Ha'apai Eruption and Tsunami: Tonga Global Rapid Post-Disaster Damage Estimation (GRADE) Report*. Washington, DC: World Bank. https://thedocs.worldbank.org/en/doc/b69af83e486aa652d4232276ad698c7b-0070062022/original/GRADE-Report-Tonga-Volcanic-Eruption.pdf