Sovereign AI

From Single Vertical to Pluralistic Ecosystem

Tom Barraclough

Brainbox Institute | March 2026

My Starting Position

⚠️ **Skeptical of 'sovereign AI' if it means:**
A single new foundation model built by government, or total supply chain isolation

But sovereignty doesn't have to mean that.

🌐 **Sovereignty ≠ nation state only**
Also communities, institutions, iwi, organisations
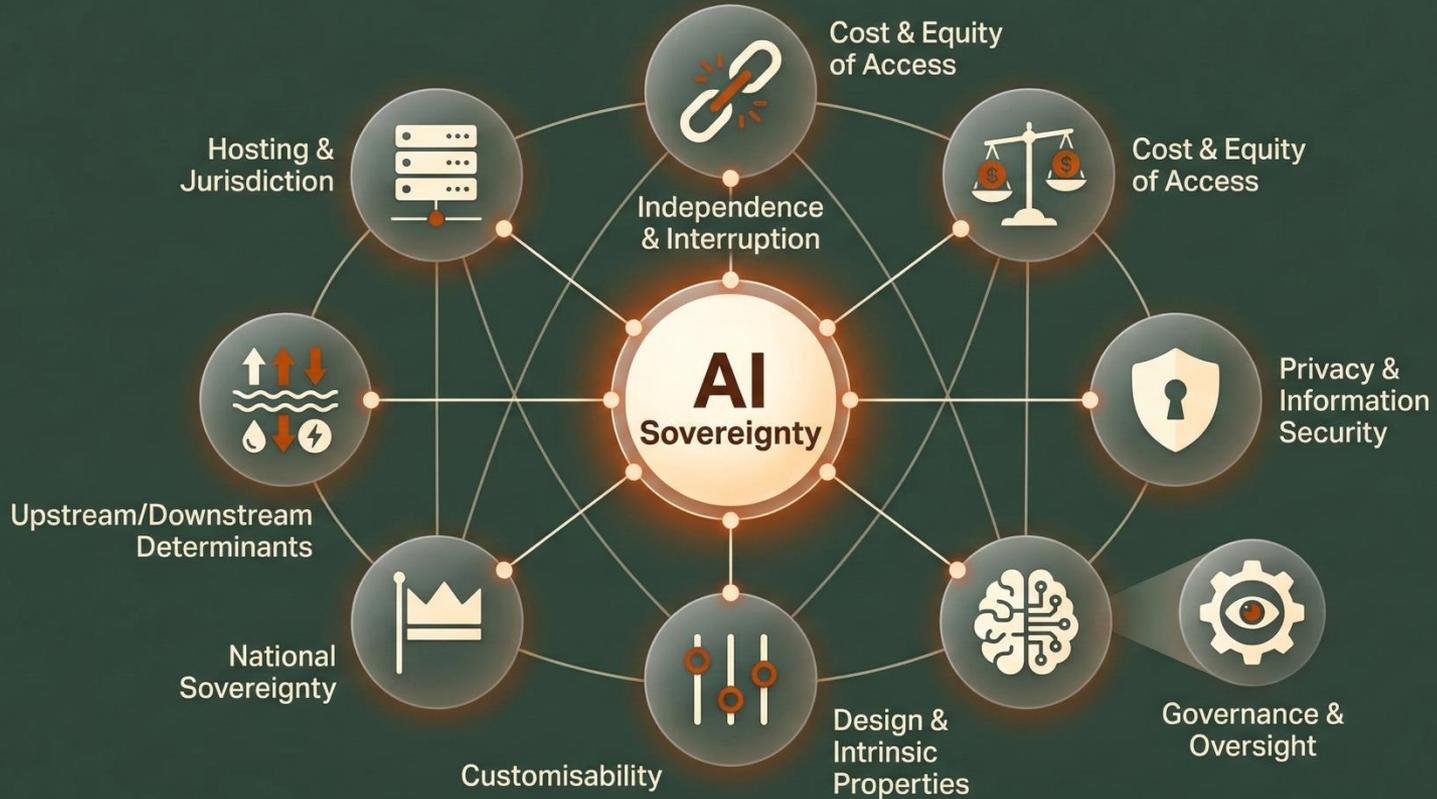
🖧 **Sovereignty ≠ isolationism**
Strategic interdependence, not isolation

▤ **Sovereign model ≠ new foundation model**
Fine-tuning, customisation, and context matter more

"Sovereignty factors"

What Could Sovereign AI Mean?

Domestic Compute & Hosting
A sovereign model hosted overseas or that no one can access is not sovereign. CLOUD Act jurisdiction matters.

Fine-tuning & Customisation
A sovereign model with little local awareness is not sovereign. Local context is essential.

AI Literacy & Capability
A sovereign model that everyone uses incorrectly or can't deploy is not sovereign.

Sovereign Context & Data
Data portability and sovereign data pipelines are key enablers. (Thanks to Chris Riley.)

Then Maybe New Models -- or Several
Only after the foundations are in place. And pluralism over monolith.

The Growing Conversation

Brookings / CEPS

Is AI sovereignty possible? Autonomy vs interdependence

Stanford HAI

AI sovereignty's definitional dilemma

WEF + Bain

Strategic investment pathways to competitiveness

Donahoe & Komaitis

Sovereignty depends on interoperability standards

Tony Blair Institute

UK strategy: sovereignty, security, scale

TPDI (Australia)

From sovereignty to agency -- a practical tool

PublicAI Network

AI as public infrastructure for the common good

EuroStack

A European sovereign technology stack

In the NZ Context

MBIE AI Research Platform

Up to $70M over 7 years for AI research infrastructure under NZIAT

NZ Tech Data Centres Report

Mapping the current state of national data centre infrastructure

Local Compute Reality

Very limited GPU access -- one set by FutureVerse (in liquidation), some at University of Auckland

Internet Resilience

Multiple recent outages, subsea cable geopolitical concerns, connectivity fragility

Content Moderation Challenge

Government-aligned content moderation raises free expression concerns, role of te reo Maori, treaty settlements

The 'Single Vertical' Problem

A single vertical orchestrated by government requires lining up an astonishing sequence of factors:

Human capability & talent	Data collection, IP & consent	Data curation & lifecycle
Training & content moderation	Fine-tuning & optimisation	Compute & infrastructure
Energy & water usage	Legal compliance & liability	Corporate governance & cyber
Access control & deployment	Funding & economic trade-offs	Future model innovation

⚠ **This sequence is politically fraught and can almost certainly never be aligned.**
Centralised funding gridlock. Content moderation by government raises free expression concerns. Every layer is complex, contested, and politically fraught.

The Alternative: Horizontal Layers, Multiple Verticals

Treat Sovereign AI not as a single vertical but as a set of horizontal layers, with multiple verticals running through them at some or all levels -- allowing for pluralism, specialisation, distribution of risk and costs, and an ecosystem approach.

Pluralism

Multiple players at each layer, not one monolithic owner

Specialisation

Actors focus where they add value, not forced across every layer

Distribution of Risk & Cost

No single point of failure, no single funder bearing all trade-offs

Ecosystem Approach

Federated governance, shared infrastructure, diverse funding streams

Sovereign AI cuts across domains:

| Social | Human | Economic | Infrastructural | Environmental | Institutional | Digital |

Monolithic vs Ecosystem

Conceptual Recreations of Sovereign AI Architectures
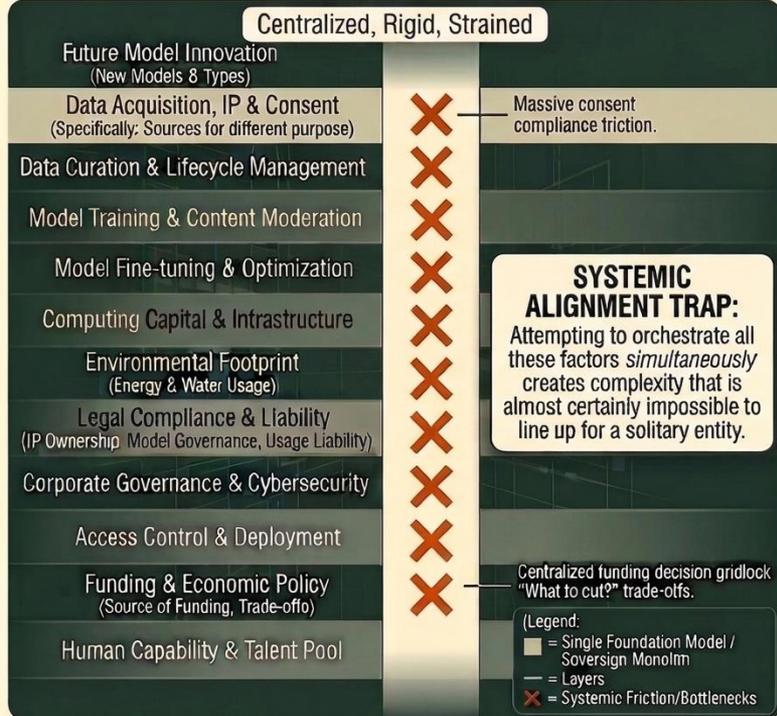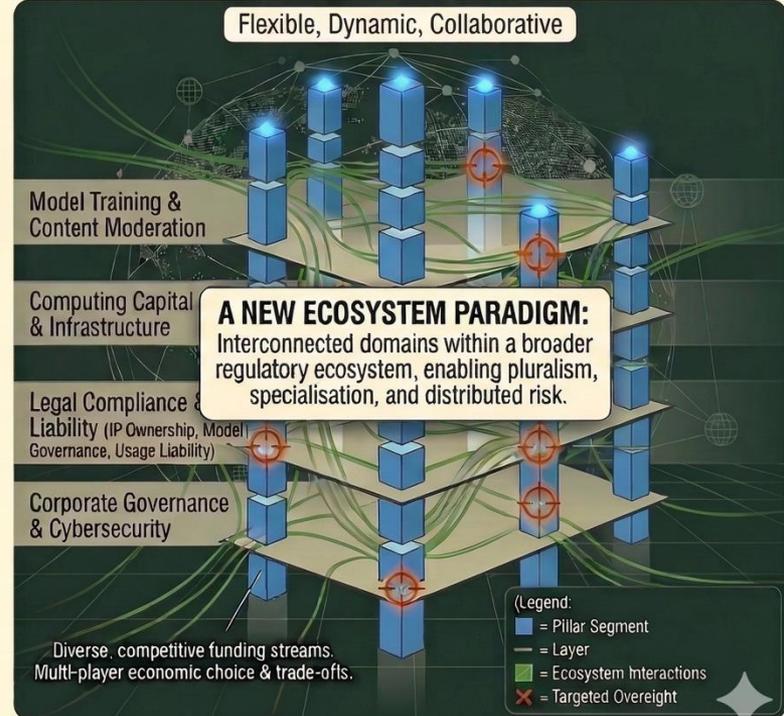
Sovereignty Factors vs NZ AI Policy

Semantic search across 210+ documents in 3 DocRef MCP knowledge graphs (149,000+ nodes)

🔍 NZ AI Policy (130,444 nodes) | DocRef (9,432 nodes) | GCDO Generative-AI Guidance

1	Hosting & Jurisdiction	**Very strong**
2	Independence & Vendor Lock-in	**Strong**
3	Cost & Equity of Access	**Strong**
4	Privacy & Information Security	**Very strong**
5	Governance & Oversight	**Very strong**

6	Design & Cultural Alignment	**Moderate**
7	Customisability	**Moderate**
8	National Sovereignty / te Tiriti	**Very strong**
9	Upstream & Downstream	**Strong**
10	Literacy, Infrastructure, Fine-tuning	**Strong**

Top sources across dimensions:

GCDO Cloud Jurisdictional Risk Guidance (DIA) | AI Playbook for Small States (Singapore MFA) | Algorithm Impact Assessments (Stats NZ) | Governing AI for Humanity (UN)
Engaging with AI (Five Eyes+) | Global Privacy Assembly Resolution | NZ Cyber Security Strategy 2026-2030 (DPMC) | **21 key documents total**

Key gap: Fine-tuning & customisation -- limited results. Nobody has properly tested what fine-tuning can achieve in the NZ context.

Five Enablers

1 **Coordination**
A coordinating vision that thinks about AI as a system. Touches nearly every area of domestic and international politics.

2 **Information**
Surface the relevant picture. What is the state of access to compute locally? Build shared situational awareness.

3 **Whole-of-Society Collaboration**
Can't have large well-resourced players moving slowly while small high-value players frantically try to keep up.

4 **Regulation**
Provide certainty and stability. Democratic ways of navigating trade-offs. Build social licence for AI deployment.

5 **Accountability**
Someone needs to take responsibility for making this work and be given the mandate to pull it all together.

Sovereign AI is a Team Effort

A soft launch: expanded AI Policy Tracker, machine-readable datasets, graphRAG MCP server -- now being used for research and writing.

Tom Barraclough
Brainbox Institute

brainbox.institute | docref.org