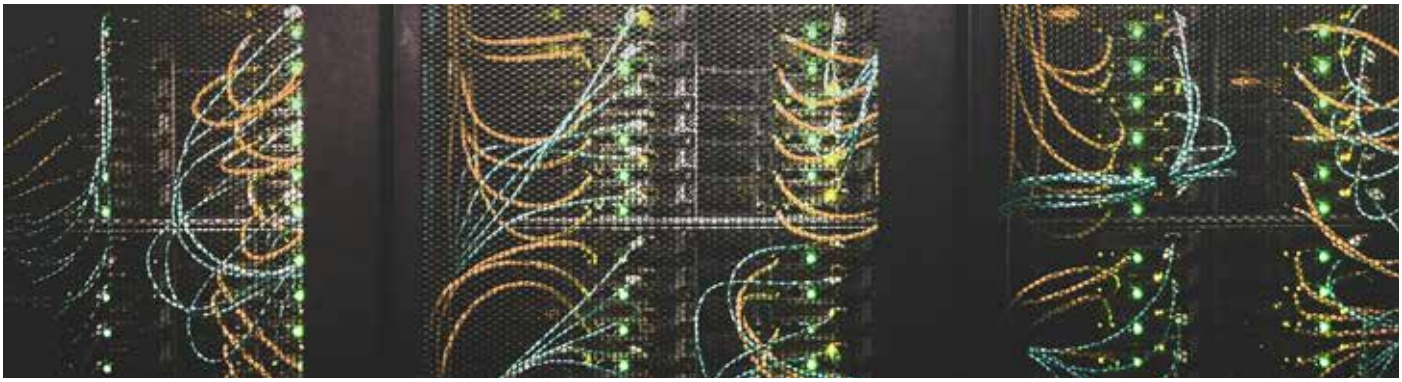
Tomorrow's Data, Today's Decisions

Think Piece 46: January 2026



Arne Larsen

This think piece explores the current and future state of data centre infrastructure in New Zealand. The operation of these centres is often overlooked, yet protecting our data is critical for ensuring the security of New Zealand. Protecting these centres will become increasingly critical with the global growth of artificial intelligence (AI) and digital services. This is the fourth think piece in the McGuinness Institute's *SecurityNZ* series.

In 2025, I had the privilege of attending both the Aspen-Otago National Security Forum 2025 (hosted by the Aspen Institute New Zealand) and The Sydney Dialogue (hosted by Australian Strategic Policy Institute). This think piece builds on some of the discussions that took place at these two events.

This think piece examines the current landscape of New Zealand's data centres and the infrastructure that underpins them. Its purpose is to contribute to ongoing discussions about data centre development in New Zealand, highlighting opportunities to strengthen the resilience of the nation's data systems and to consider if there is value in positioning New Zealand as a competitive destination for hosting international data. Although domestic data needs and commercial opportunities are distinct, they are closely interconnected and should be addressed within a single overarching strategy, as both rely on largely the same underlying infrastructure.

This think piece does not analyse the cost of capital, the operational costs of running data centres and managing shared infrastructure (such as cables), or how water and power costs may evolve in the near future. These are important considerations that warrant separate, detailed analysis.

The paper calls for a comprehensive strategy to be developed in stages. The first stage is a detailed assessment of the data New Zealand holds that is of national significance, with the aim of identifying where resilience can be improved. The second stage is an in-depth evaluation of whether there is a viable commercial opportunity to invest in infrastructure to attract international investment, and, if so, what the associated costs, risks, and benefits would be for New Zealanders. Figure 1 (overleaf) identifies some major trends for consideration.

AI is one of the leading drivers of growth in demand for data centre capacity, with demand for data centres projected to triple by 2030.[1] This will lead to competition for the critical resources required to build the centres, as well as the large amounts of power and water required to run them.[2] As power becomes more expensive and water more scarce, data centre owners and operators will look to countries where there is plentiful renewable energy and water – countries like New Zealand.[3]

Quantum computing is another key trend. Data centres will need to be designed to facilitate new hardware, lower operating temperatures, differently skilled personnel, and more secure security systems.[4] Interestingly, New Zealand is right at the forefront of quantum research. On 8 December 2025, the Ministry of Business, Innovation & Employment (MBIE) announced that three New Zealand universities would be partnering with universities in the Republic of Korea to advance quantum communication technology.[5]

I: DOMESTIC DATA NEEDS

The landscape is evolving rapidly, making it essential to answer three key questions about our domestic data.

(i) Where does New Zealand store its data?

New Zealand largely relies on data centres that are located overseas and owned by private, often multinational, companies. A 2022 report by Te Kāhui Raraunga discussed the current state of government data storage and revealed that, increasingly, government departments were storing their data in overseas data centres.[6] The report argued that more consideration must be given to Māori data sovereignty and security.

In response to the McGuinness Institute's OIA 2025/07, the Department of Internal Affairs (DIA) advised that not all government data is stored in New Zealand, and that DIA does not hold a list of the locations or ownership of data centres that store New Zealand government data.[7] DIA also included a list of eight data centre providers that have entered into cloud and software framework agreements. See Table 1 (below).

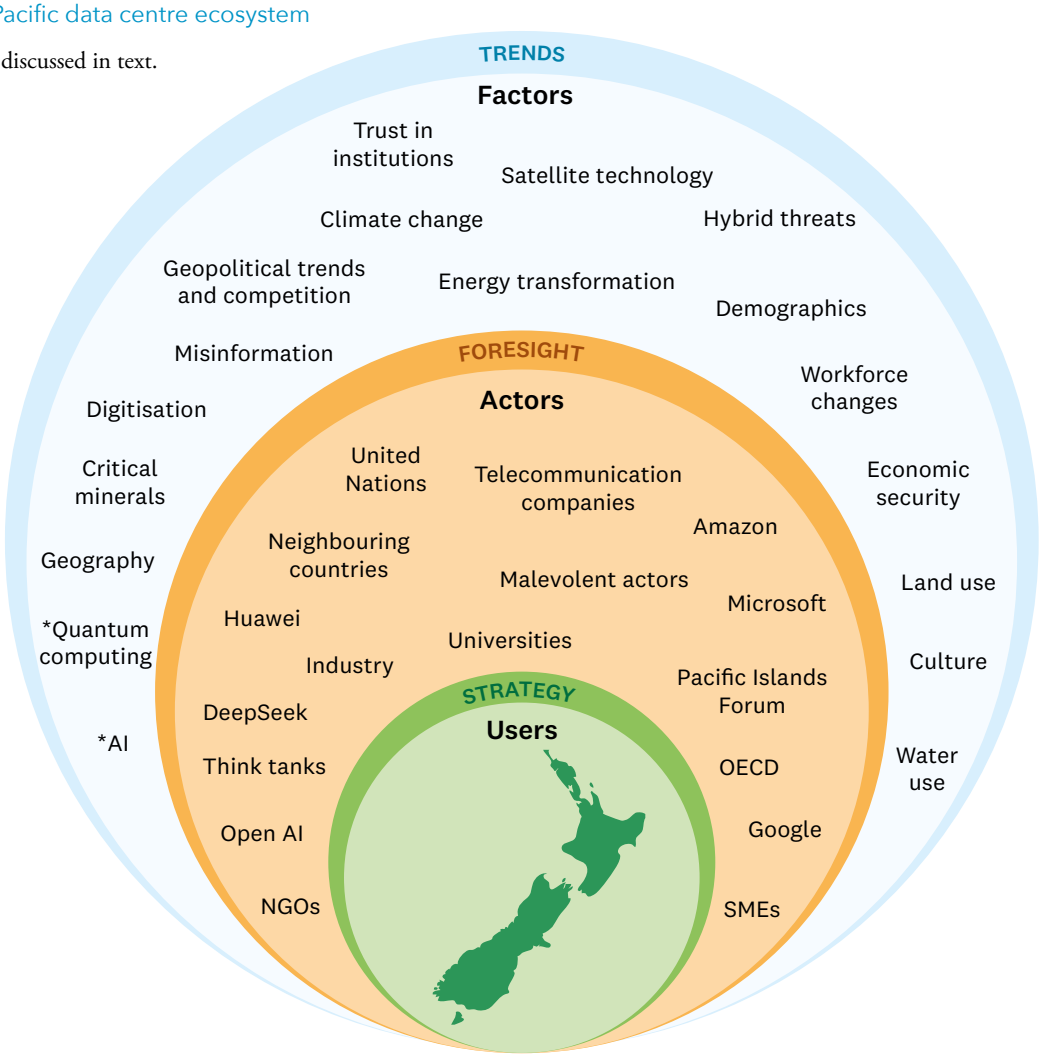
Table 1: New Zealand government cloud and software framework agreements with data centre suppliers

Source: Adapted from DIA, personal communication, 14 July 2025[8]

Cloud supplier	Location of company	Location of data centre	Other data centres
Amazon Web Services[9]	United States[10]	Auckland[11]	Yes, various[12]
CatalystCloud[13]	New Zealand[14]	Porirua, Hamilton and Wellington[15]	No[16]
Datacom[17]	New Zealand[18]	Auckland, Wellington, Hamilton and Christchurch[19]	Yes, in Sydney and Melbourne[20]
Google[21]	United States[22]	Not in NZ[23]	Yes, various[24]
Microsoft[25]	United States[26]	Auckland[27]	Yes, various[28]
SAP[29]	Germany[30]	Not in NZ[31]	Yes, various[32]
TechnologyOne[33]	Australia[34]	Not known	Not known
Oracle[35]	United States[36]	Not in NZ[37]	Yes, various[38]

Figure 1: The Indo-Pacific data centre ecosystem

Key: * These trends are discussed in text.



Recently, several privately owned data centres have been developed in New Zealand. Microsoft was the first 'hyperscaler' to open a data centre in New Zealand, in Auckland in December 2024.[39] In September 2021, Amazon announced plans to construct new data centres in Auckland but ultimately chose to invest in a cluster of existing facilities instead.[40]

In response to the Institute's OIA 2025/07, New Zealand's Government Communications Security Bureau (GCSB) advised that in May 2025, it took control of an all-of-government data centre hosted on a New Zealand Defence Force base in Auckland.[41] This centre is not intended to store all of the government's data, only 'the most sensitive information held by a number of public sector agencies'. The GCSB also advised that New Zealand's most sensitive data is stored within New Zealand in line with current protective security requirements.[42]

(ii) How does New Zealand access our data?

New Zealand relies on both undersea cables and satellites to stay connected. New Zealand is currently connected through four international undersea cables, with a further three set to be completed in the next few years.[43] These seven cables will connect New Zealand with American Sāmoa, Australia, Fiji, French Polynesia, Kiribati, Tokelau, Tonga and the United States.[44] Undersea cables currently carry 99.7% of New Zealand's internet traffic – undersea cables offer much more capacity than satellites.[45] Cables deliver data like a fire hose; satellites, by comparison, are a straw.

Unfortunately, undersea cables are prone to breaking. Globally, an average of two to four cables break every week. Generally, these are accidental breaks from anchoring or fishing, or natural disasters like undersea earthquakes and landslides.[46]

As global shipping activity has increased, so has the incidence of cable breakages. A growing threat internationally is cables being purposely cut to disrupt critical undersea infrastructure.[47] Resilience can be gained through building more cables in different geographic locations, so if a cable does break, data can be rerouted through other cables with minimal impact.[48]

Satellite-to-satellite communication is another option for accessing data in New Zealand. Currently satellites are used only as a back-up if a cable breaks and a temporary solution is needed. For example, after a volcanic eruption took out an undersea cable in Tonga, the Pacific nation used satellites to maintain communication across the islands.[49] Because of the number of small communities across thousands of islands in the Pacific region, it would be inefficient to connect multiple submarine cables across each island, so it is likely that Pacific nations will invest further in satellite connectivity.[50]

New Zealand currently has six Starlink ground stations, required to access the satellite constellation, and as at September 2024 New Zealand had the highest uptake of satellite communication per capita across the OECD (14% of New Zealand's rural community use satellite communication).[51]

(iii) What are the implications (e.g. in 5, 15 or 30 years)?

An assessment of the strengths, weaknesses, opportunities and threats associated with New Zealand's domestic data needs can enable valuable foresight into policy and security implications. A critical part of this analysis is distinguishing between what is known and what remains uncertain. For instance, it is not yet clear whether future investment will prioritise large hyperscale centres, smaller regional facilities, or more distributed edge networks. Table 2 (overleaf) is a high-level assessment of the current, and likely future state of data centre infrastructure.

Table 2: An assessment of the strengths and weaknesses of the current system and the opportunities and threats ahead

Infrastructure type	Strengths	Weaknesses	Opportunities	Threats
Offshore data centres	• More cost-effective for New Zealand, as we don't have to build our own.[52] • Greater security in case of disaster or an attack on New Zealand.[53]	• May be subject to data laws of other countries (e.g. the CLOUD Act).[54] • Data sovereignty could be compromised.[55]	• A data embassy could be considered in an ally's territory, allowing for data sovereignty overseas.[56] • New Zealand could consider undersea data centres (e.g. see China's pilot project)[57] or space-based data centres for more efficient cooling/ power.[58]	• Geopolitical tensions may result in more attacks on data centre infrastructure; centres we rely on overseas could be attacked.[59] • Cyberattacks or physical attacks could damage data centres; centres we rely on overseas and locally could become compromised.[60]
Onshore data centres	• Greater control over where our data is located, which will be particularly valuable when it comes to protecting data critical to New Zealand.[61]	• Higher costs associated with building the centres. • Potential negative environmental impacts, including e-waste and changes in water usage.[62] • May be subject to data laws of other countries (e.g. the CLOUD Act).[63]	• New Zealand's access to renewables could attract investment , enabling us to become a sustainable data centre superpower.[64]	• Power and water costs are a barrier to any new data centres in New Zealand.[65] • Climate change is impacting on water availability and power costs internationally and domestically. For example, hyperscale data centres could strain existing water supplies.
Cable lines	• Can rely on private sector to build and maintain, as it is in their best interests to ensure effective cables.[66] • Building more is the best resilience, as the more cables we have, the less likely it is that they will all break.[67] • Cables have enough redundancy that if any one cable goes down the data will be rerouted.[68]	• Because they go through international waters, there are some issues with New Zealand's ability to regulate.[69] • New Zealand relies on private-sector expertise and ships to lay, repair and manage cables.[70] • There is only one ship, the CS *Reliance*, that is responsible for maintenance of cables in the South Pacific region. • Cable suppliers must be vetted to ensure cables are not compromised.[71]	• More cables mean more resilience: continuing to build and allow the building of cables makes New Zealand more resilient to breaks.[72] • New Zealand could aim to become a critical hub for submarine cables in the South Pacific, as Singapore has done.[73]	• Climate change impacts can damage the landing sites.[74] • Natural disasters such as undersea landslides, earthquakes and volcanoes can damage cables.[75] • Cables can be cut, either purposely or accidentally.[76] • Hostile actors could hack into cables, either undersea or at the landing points.[77]
Satellite-to-satellite	• A back-up if cables are broken. Allows important data to be accessed if necessary.[78] • Protected from many natural hazards that cables can be damaged by.	• Cannot transport as much data as cables.[79]	• Growth in New Zealand's space industry could allow for New Zealand-owned satellites and constellations.[80]	• Satellites could be damaged by debris in space – the likelihood increases with the growing number of satellites in orbit. Low earth orbit is a finite area, and the more satellites are there, the more likely collisions become.[81] • Satellites can be compromised through physical damage or through cyberattacks.[82]

II: INTERNATIONAL OPPORTUNITIES

After developing a detailed understanding of our domestic needs, but before determining the way forward, it is necessary to assess whether commercial opportunities exist, such as hosting international data in data centres located in New Zealand. These facilities could be either New Zealand-owned or internationally owned.

What is clear, is that the world is becoming more digital, and the global demand for data centres will continue to increase. New Zealand, with its abundant renewable energy and water resources, may be able to position itself as a beneficiary of this growth.[83]

Several options exist. Below, we briefly discuss three.

(i) Become a regional hub, like Singapore. This will require investment and regulation in both communication infrastructure (e.g. cables and satellites) and renewable energy and water resources. Large multinational companies may also be interested in setting up offices in New Zealand, due to our proximity to the Pacific, but also to support research in Antarctica.

(ii) Encourage hyperscalers to invest in infrastructure. For example, invest in renewable energy generation and upgrading the power grid to support a higher load, which are both key investments that they would likely need to invest in regardless. Mapping out how they could support developing the infrastructure would provide these hyperscalers with some certainty regarding New Zealand's commitment to digitisation.

(iii) Cooperate more with Pacific Island nations. This could follow a model similar to Australia's partnership with Papua New Guinea (PNG), where Australia, alongside the United States, is supporting the development of PNG's digital infrastructure.[84] Another option would be to establish data embassies for Pacific nations in New Zealand. Estonia provides a useful precedent: it has created a data embassy in Luxembourg, a state-owned facility that holds the same legal status as a foreign embassy and can be accessed quickly in the event of an emergency.[85]

All three of the above options would attract talent to New Zealand, to build the infrastructure itself and to conduct research into AI and quantum computing technologies.

Developing a clear strategy and detailed roadmap would give partners confidence in New Zealand's long-term data approach while deepening collaboration with hyperscalers seeking a stable, cost-effective investment environment and with Pacific Island neighbours seeking guidance, partnership, or security.

Maintaining a strong and coherent data-management brand will be essential if we want to position New Zealand as a trusted and strategically aligned destination for future business opportunities. What is clear, however, is that building a deep understanding of the sensitive data we value and the protections it requires, alongside investing in supporting infrastructure and partnering with like-minded, standards-focused organisations and countries, will be critical to achieving this.

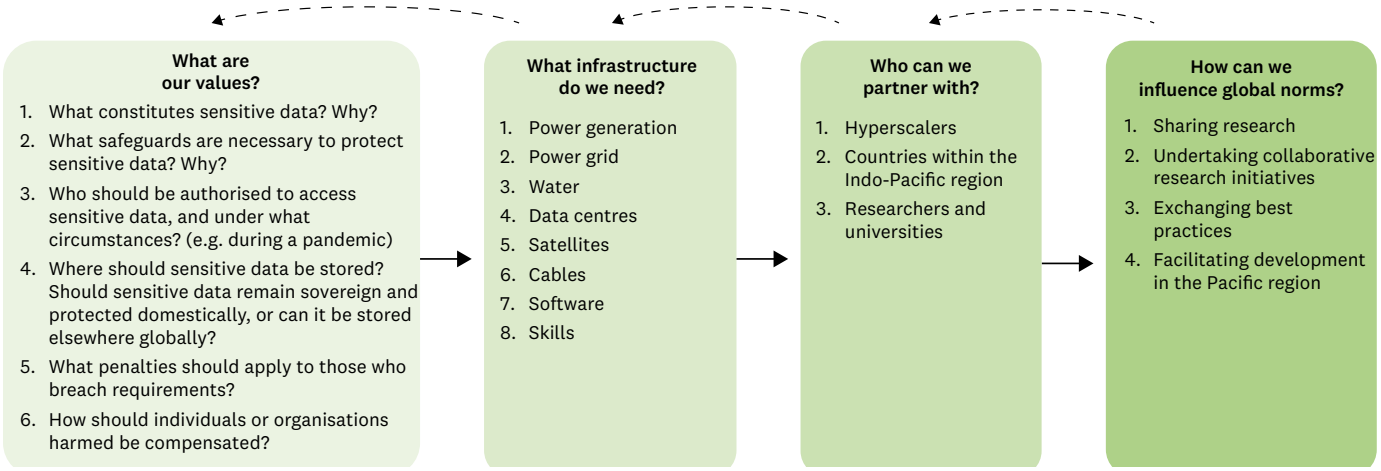
Regardless of the path we choose, global norms and standards will continue to be shaped by those developing the technology. The window to influence these norms is small and narrowing, underscoring the need for New Zealand to build the talent and skills required to remain informed, capable, and responsive in a rapidly evolving environment.

RECOMMENDATIONS

Below are eight suggestions on the way forward:

1. **Create a sensitive data taxonomy.**
   While there is strong focus on sensitive security data (where disclosure could cause harm, enable misuse, or compromise security) and sensitive private data (where disclosures would harm an individual), there appears to be far less attention on sensitive market data (where disclosure could affect market behaviour, reduce public trust, distort competition, or harm an organisation's/country's commercial interests) or sensitive public data (where disclosure would harm democracy).
2. **Determine the type of protections that are required for each type of sensitive data (in 1 above).**
   As noted, sensitive data extends beyond security data, and even within sensitive security data there may be varying degrees of sensitivity. Given this, further work is required to develop a comprehensive and coherent system of protections for all forms of sensitive information.
3. **Develop strong international relationships.**
   Build relationships with standard-setters, technology providers and countries that we can trust to supply and build the cables and data centres. This includes collaborating with international security partners. Similarly, we should ensure that the data centres we use overseas are trustworthy.
4. **Adopt a principle of geographic diversity.**
   Ensure geographic diversity, both nationally and internationally, in both cable types and landing locations, as well as satellite pathways, to strengthen New Zealand's resilience against breakages and other disruptions, including malicious activity and solar events.
5. **Invest in back-up options to protect New Zealand's sensitive data from potential threats**.
   This may involve building/expanding undersea cables, satellite launch sites and government data centres. Building more cables provides most resilience, as the more cables we have, the less likely they would all be broken at once.
6. **Strengthen cybersecurity policy and strategy.**
   This includes carefully protecting where sensitive information, such as New Zealand government data, is stored. It also requires encryption of data, regularly checking for potential risks in the system, knowing clearly what data is critical for New Zealand, and ensuring this data is held locally in a secure data centre. Countries around the world are aware that technological advancement will translate into geopolitical advantage; by being the first to develop a piece of technology, countries are able to set the global norms and regulate how the technology is used.
7. **Focus on a sustainable and local energy system**.
   This includes developing new technology, upskilling the workforce and investing in green energy such as hydro, wind and geothermal. This will encourage foreign investors who are interested in building data centres and undersea cables.
8. **Monitor threats to data security.**
   This includes regular testing for weaknesses in the system and collaborating with international partners to understand possible risks and how we can protect ourselves.

Figure 2: Pathway to a data centre strategy for New Zealand



The McGuinness Institute is a non-partisan think tank working towards a sustainable future, contributing strategic foresight through evidence-based research and policy analysis.
McGuinness Institute, Level 1A, 15 Allen Street, PO Box 24222, Wellington 6142
Phone: (04) 499 8888 Email: enquiries@mcguinnessinstitute.org Website: www.mcguinnessinstitute.org