Risks and Challenges of Non-Domestic Data Centres for Isolated Countries

A dissertation

submitted in partial fulfilment

of the requirements for the Degree

of

Master of Cyber Security

at

The University of Waikato

by

Peter Wanyonyi

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

2025

Abstract

Small and isolated nations have been significant early adopters of Cloud Computing services, driven in part by the potential for cost savings and the convenience of not having to build their own Internet and computing infrastructure. This move into the Cloud has not been without challenges - indeed, while these services offer scalability, flexibility, and cost-efficiency, they also expose these nations to unique risks and vulnerabilities. Many of these nations are at significant distances from the Data Centres whose services they consume, introducing unavoidable transmission challenges as well as legal and geopolitical issues for these nations, given their lack of control or enforcement capability over the foreign-hosted data centres whose services they consume.

As case studies, in this work we identify, measure and investigate some of the technical challenges posed by reliance on foreign Cloud Data Centres, and also analyse and discuss the non-technical challenges faced by nations that rely on such facilities. In those case studies, this work also explores how small and isolated nations can navigate these challenges, and recommends courses of action that provide actionable options for such nations. This dissertation also examines the disadvantages and risks associated with the reliance on non-domestic data centres by small, geographically or politically isolated nations where studies of such characteristics are possible, such as New Zealand and Taiwan.

Acknowledgements

I would like to thank Professor Marinho Barcellos for his guidance and patience in the development of this dissertation.
I would also like to thank Mercury Energy Ltd for providing me with the time and facilities to carry out the measurements described in the dissertation.
Finally, I would like to thank my family for their support. To Lucille, Grace, Natasha, Peter - not forgetting Tabby and Rambo! - I am grateful for your unwavering support and encouragement, and for your patience and understanding during the long hours spent working on this project[1].

[1]This work has been carried out and developed by the author, and the writing is original and is not copied from any other source except where indicated in the citations as a source. The author did not utilise any ghostwriting services, AI, or any other form of writing assistance in the development or writing of this work.

Contents

Chapter 1

Introduction

1.1 Problem Statement and Motivation

Reliance on Internet Cloud services is an observed feature of both business (Dillon & Vossen, 2015) and government IT infrastructure (Kumar et al., 2024) in small and/or isolated countries. This is driven by the need to minimise costs (Dillon & Vossen, 2015) while increasing technology services responsiveness flexibility for both governments and businesses (Mather et al., 2009). Geographically or geopolitically isolated locations make it more economically feasible (Mather et al., 2009) for such countries to utilise Cloud infrastructure based in other jurisdictions. IBM Cloud in New Zealand, for example, is serviced from IBM's Sydney Data Centre ('IBM adds watsonx service to IBM Cloud in Australia and New Zealand', 2024). Similarly, until 2024, Microsoft's New Zealand Region was actually serviced from Australia (Sorenson, 2024). The relatively straightforward access to Cloud services makes this model of computing and Cloud access take precedence over investing in domestic data centres. Such dependence can expose small and isolated countries to challenges that include technical (Phaphoom et al., 2015), economic, legal (Cory, 2017),and geopolitical (Zheng & Gong, 2024) issues.

Incidences of Cloud Service disruptions are growing in frequency and severity. These are caused by a variety of factors, including natural disasters,

cable cuts, government-ordered shutdowns, and suspected hostile action by nation-states (Wu et al., 2024). (Gamero-Garrido et al., 2021) found that many countries are particularly exposed to Cloud service disruption, data traffic observation or tampering due to their traffic being routed through centralised infrastructure. Frequently, this infrastructure is located in other countries, and is thus subject to the laws and regulations of those countries. This can lead to data sovereignty issues, where data is stored in a foreign jurisdiction, and can be accessed by foreign governments (Cory, 2017).

Geopolitical tensions are also becoming more frequent, and are driving up Internet service disruptions. These take various forms, including traffic manipulation, intentional rerouting of data traffic, and throttling, and are frequently out of the control of the affected countries (Wu et al., 2024). Where geopolitical tensions and hostile actions by nation-states are underway, the methods used to disrupt Internet services can involve both technical measures and military tactics, such as forcing Internet companies to hand over infrastructure control or data. This is made worse in cases where the affected country relies on Internet infrastructure or Cloud services owned by or based in other countries, as seen during Russia's takeover of parts of Ukraine in 2022-2024 (Times, 2022).

Asserting Data Sovereignty is a challenge when a country relies on foreign-hosted Cloud services. This is compounded by legal differences between the subscriber country and the host country, and can lead to difficulties in enforcing national cyber laws (Cory, 2017). To address this, some countries have enacted data sovereignty laws that require data to be stored within the country's borders (Cory, 2017), or which restrict or otherwise limit the cross-border flow of data and information (Cory, 2017). Countries that do not have their own data centres or Cloud infrastructure are at a disadvantage in this regard, as they have no choice but to rely on foreign-hosted Cloud services.

Although these factors are well-known, there are few works that bring all the factors together and view them as a combined set of challenges - technical,

geopolitical, legal, and security - from the perspective of small and isolated countries. This work aims to help begin to fill this gap by providing a comprehensive view of these challenges as faced by small and isolated countries that rely on foreign-hosted Cloud services. Because the challenges fall in several different areas, this work will focus on the technical challenges of network performance, and will also discuss the other challenges and how they affect small and isolated countries. The categories in which these challenges fall are as follows:

- Performance degradation due to cable cuts or distance, such as happened in Kenya due to cable cuts in the Red Sea on February 24, 2024 (Payton, 2024);
- Increased vulnerability to geopolitical tensions resulting in Cloud service disruptions, such as has happened severally in Northern Europe recently (Aggarwal, 2025);
- Difficulties in enforcing national cyber laws because their data is stored offshore in other legal jurisdictions, thereby compromising their digital sovereignty and economic resilience (Galij et al., 2024).

This work discusses these and related challenges, and provides recommendations on how small and isolated countries can navigate them.

1.2 Dissertation Outline

The rest of this work is structured as follows: Chapter 2 provides a background on the challenges of relying on foreign data centres for Cloud services. Chapter 3 reviews the literature on the performance, geopolitical, legal, cybersecurity and other challenges of foreign-hosted Internet services. Chapter 4 details the measurement of network performance metrics as observed from New Zealand and Australia to offshore data centres, and also discusses the other

risks of relying on foreign-hosted Cloud services. Chapter 5 discusses the results of the observed metrics as well as those of the other challenges. Finally, Chapter 6 provides recommendations and conclusions, while Chapter 7 is an appendix of the technical and industry terms used in this work.

Chapter 2

Background

This chapter presents the necessary background to the challenges addressed in this dissertation. It reviews each of the identified challenges presented by the use of non-domestic Cloud data centres and discusses their nature and implications for isolated nations.

2.1 Isolated Countries and Cloud Services

The phrase **"Isolated countries"**, within the scope of this dissertation, refers to countries that experience significant geographical remoteness or geopolitical seclusion, both of which adversely affect their access to global digital infrastructure and services (Hudson, 2011). This definition sometimes overlaps with that of "small states" in the geopolitical and economic sense, when defined from the perspective of geography or population (Bhatta, 2023), although some small states (e.g. Singapore) are not isolated, while some large states (e.g. Congo DRC) can also qualify as isolated. This dissertation focuses on the isolated states – those whose connection to the outside world is tenuous at best (Bhatta, 2023).

This isolation can be the result of physical distance from major economic centres (for example, New Zealand and many African countries) or of political circumstances that limit international engagement and make those countries susceptible to digital isolation as a result – for example, Taiwan (Msongaleli

et al., 2015) and Cuba (Bhatta, 2023).

As with the rest of the world, isolated countries have adopted or are looking to adopt Cloud Services due the global push towards digital government, digital sovereignty, and economic connectivity (Kumar et al., 2024). This is despite many of them not hosting any data centres from the major cloud providers such as Microsoft Azure, AWS, or Google Cloud (Dillon & Vossen, 2015). In geographically-isolated New Zealand, for example, many organisations have been moving their workloads to the cloud to leverage the benefits of scalability, cost-efficiency, and accessibility (Tongsuksai et al., 2023). This means those organisations store their data in cloud data centres based in Australia, Singapore, the UK, the USA, and other countries around the world that host Cloud data centres (at the time of writing, New Zealand is about to get its first domestic Cloud data centre (Sorenson, 2024)).

In Law Enforcement, lack of local data centres can impede the enforcement of national cyber laws and data sovereignty (Koske et al., 2014). This is because when data is stored abroad, it becomes challenging for governments to assert legal authority over it, leading to potential conflicts between national interests and foreign jurisdictions (Pohle & Thiel, 2020). This lack of legal jurisdiction over offshore data centres can be exacerbated by the difficulty of ensuring the adherence of large Internet Cloud companies to local laws.

The last few years have seen an increase in the *centralisation* and *consolidation* of Internet services in the hands of a few very large Internet companies – the so-called "hyper-giants" (Moura et al., 2020). These hyper-giants provide platforms that host various services for end users, including free web email, Social Media, Identity Services, and so on. They include Microsoft, Google, Meta (which owns Facebook), and X (formerly Twitter) (Koske et al., 2014). The hyper-giants are characterised by their collection of vast amounts of data about users, which they store in data centres worldwide, usually in a select few countries where they are protected from oversight (Koske et al., 2014). This can result in inadequate protection of citizens' data privacy and security, as in

the cases illustrated below:

- **Brazil:** The recent conflict between X (formerly Twitter) and the Brazilian government, particularly the role of Elon Musk in shaping corporate policy that disregards national laws around data privacy and content moderation (The Guardian, 2024).
- **Australia:** The standoff between Facebook and the Australian government over the News Media Bargaining Code, where Facebook temporarily blocked news sharing in retaliation against legislative efforts to force the platform to compensate news publishers (Australian Competition and Consumer Commission, 2021).
- **Canada:** Facebook's struggle with Canada's proposal to implement similar laws to Australia, with the focus on the tension between local news industries and Internet hyper-giants (BBC News, 2024).

The dependence on non-domestic data centres by isolated countries introduces a spectrum of challenges, including performance issues, heightened geopolitical risks, increased costs, and compromised legal authority over data. Addressing these challenges, as discussed in the next sections, is crucial for enhancing the digital resilience and sovereignty of these countries.

2.2 Performance Degradation

For isolated countries accessing Cloud services hosted offshore, performance degradation is a significant concern. The physical distance between users and data centres invariably results in increased latency, jitter (variation of latency), and packet loss (Chen et al., 2009). This significantly impacts network performance (Charyyev et al., 2020), leading to suboptimal user experiences and hindering the adoption of cloud-based services (Maheshwari et al., 2018). For instance, users in New Zealand accessing data centres located in the United

States may experience noticeable delays due to the vast geographical separation (Inc, 2024). This often results in suboptimal user experiences when accessing Cloud services, and can make some applications – such as streaming multimedia or gaming platforms – difficult to run or even unusable (Chen et al., 2009). This performance degradation can hinder the adoption of cloud-based services and negatively affect user experience and productivity (Tongsuksai et al., 2023).

The *physical infrastructure* used to deliver Cloud services can also pose a challenge. The dependence on undersea cables for international data transmission introduces vulnerabilities for isolated nations (Msongaleli et al., 2015). Disruptions caused by natural disasters or technical failures can lead to significant service outages. The 2022 undersea cable cut that disrupted Internet services in Tonga underscores the fragility of such infrastructure and the potential impact on nations reliant on these connections for accessing cloud services (Wang et al., 2023). The reliance on non-domestic data centres exacerbates these issues, as data must traverse long distances, increasing the risk of interruptions and performance degradation (Chen et al., 2009).

As this work will later show (Chapter 4), latency appears to be based mainly on distance to the Cloud provider endpoint and the routing path used, and does not change significantly regardless of time of day or day of the week in question. This work also investigates whether cloud access from edge servers can result in significantly better latency performance than using traditional Cloud Service Providers (CSPs) directly, and if this approach can be used to mitigate the latency issues faced by isolated countries to a point (Kshetri, 2010).

2.3 Other Challenges

The geopolitical challenges that isolated countries face can be amplified by a dependence on foreign data centres. Such countries may find their data

subject to foreign surveillance or legal jurisdictions (Bhatta, 2023), potentially compromising sensitive information or treating and/or accessing data in a manner not acceptable to the original data owners (Sharma et al., 2024). Further, strained geopolitical relationships between countries can lead to significant concerns when one of those countries relies on the other for Cloud services, such as the case with Taiwan relying on China-based data centres (Jansen et al., 2023).

The resilience and reliability of data access when relying on foreign data centres is often dependent on functioning undersea cable connections, which are carried on the worldwide Submarine Cable Network (SCN) (Swinhoe, 2024). The SCN is the backbone of global Internet connectivity, and damage to the cables can isolate countries from critical data services (Tod, 2022). Recent events have highlighted the risks that geopolitical tensions can pose to the SCN ands thus to the availability of cloud-based services (Astier & Kirby, 2024). On February 24, 2024, 3 critical SCN cables in the Suez Canal were cut when the Belize-flagged carrier cargo ship *MV Rubymar* sank as a result of a suspected attack by parties involved in Yemen's civil war (Swinhoe, 2024). The anchor of the sinking ship is thought to have severed the cables, which are critical to the Red Sea SCN and are used by many countries in the region, including East and Southern African nations.

The result was significant disruption of data traffic to and from Kenya, the East African Coast (Payton, 2024). More than 40 percent of Kenya's interregional bandwidth is connected to Europe via the Red Sea SCN, and the cable cuts caused significant disruption to the country's Internet services (Swinhoe, 2024). Measurements carried out at the time showed significant slowdown in Internet speeds in Kenya and the East African region (Swinhoe, 2024), all of which persisted for over a week. Figure 2.1 shows the area in which the cable cuts occurred in the context of the regional SCN.

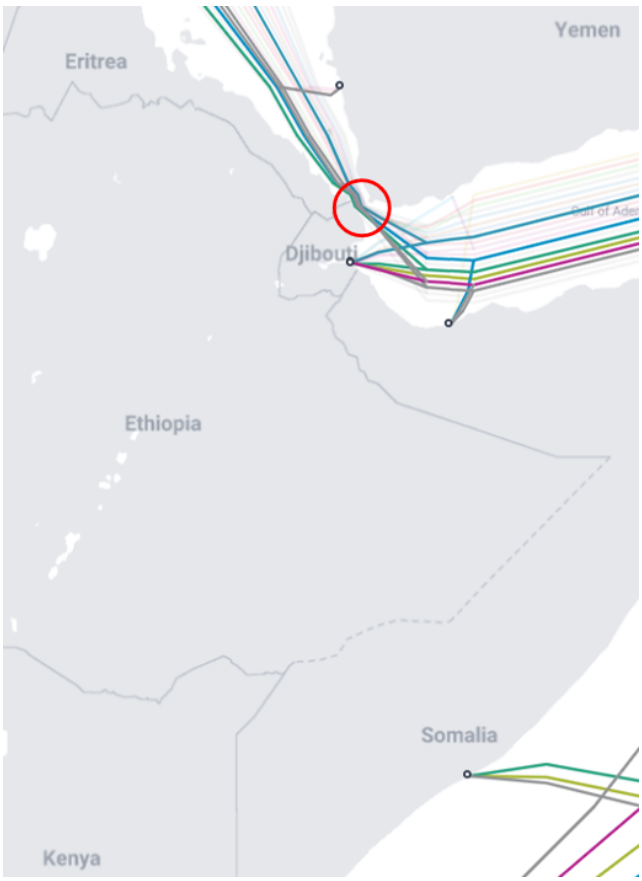

Figure 2.1: Region (circled red) where the cable cuts occurred (Telegeography, 2025a)

Further events of this nature have occurred since then, with geopolitical tensions in Europe being suspected of being the underlying causes for several SCN cable cuts in the Baltic Sea, for example (Astier & Kirby, 2024). In such scenarios, the availability of cloud-based services to the consumer could be severely impacted, posing risks to national security and the continuity and reliability of essential services (Tod, 2022). The impact of such events on isolated countries can be severe, given their reliance on foreign data centres for critical services.

Geographical challenges as a result of natural disasters can also impact the availability of cloud services to isolated countries. The December 2006 earthquake in Taiwan, for example, caused significant damage to the undersea cables connecting the country to the rest of the world, leading to widespread Internet outages (Carter et al., 2009, p. 9). Even where a country has set up its own data centres, the interconnectedness of Cloud services relies on undersea

cables that can make such a country's access to those services vulnerable, as is the case with Japan (Kobayashi, 2014) – whose digital access to the outside world is frequently compromised by cable breaks caused by earthquakes and related natural disasters (Msongaleli et al., 2015). Where a country relies entirely on foreign-hosted Cloud services, the impact is that much greater when there is disruption in the SCN serving that country.

Legal non-compliance is another risk that isolated countries face when relying on foreign data centres for Cloud services. Reliance on foreign-hosted Cloud Services can result in isolated nations having to bear the risk of legal non-compliance by foreign data centre owners. As mentioned already, in recent years the Internet has seen a growing centralisation caused by the consolidation of data traffic, users and infrastructure by a few "hyper-giants", the major Internet players (Moura et al., 2020). These hyper-giants are generally based in Western countries such as the USA and the UK/Ireland, while providing Cloud and related services worldwide – which can lead to scenarios where local laws are ignored by the hyper-giants (Jansen et al., 2023). Isolated countries without data centres in their own jurisdictions lack the means – legal, technical, or economic – to enforce their own laws as they apply to their data. They are often unable to regulate content on platforms hosted by hyper-giants in foreign jurisdictions, leading to inadequate protection of citizens' data privacy and security (El Makkaoui et al., 2015).

Data Security is a major concern in Cloud Computing (Mather et al., 2009), especially when data is stored in foreign jurisdictions (Bhajantri & Mujawar, 2019; Pohle & Thiel, 2020). Surveillance or other interference with such data can be legal in the jurisdiction where it is carried out, such as for law enforcement, or it could be covert (Schwartz, 2018). This can also result in data breaches, unauthorised access, or cyberattacks, including those from state-sponsored actors (Kushwaha et al., 2020). Where the data belongs to an isolated nation or a small economy, it would be difficult or impossible for the data to be protected from such access attempts. This risk is compounded

by the need for Cloud providers to store user data in multiple locations for redundancy – where such locations are in different jurisdictions, the security risks that apply to that data increase with the number of jurisdictions involved.

The management of governance, shared responsibilities, and implementation of security processes to data stored in the Cloud can also be a challenge, particularly given how frequently Cloud providers update their services, tools, and terms of service (Mather et al., 2009). For isolated nations, reliance on foreign-hosted cloud services can heighten the risk of data breaches, unauthorised access, and cyberattacks, including those from state-sponsored actors (Kushwaha et al., 2020). Differences in cybersecurity protocols between jurisdictions further expose such data, especially when sensitive, to vulnerabilities. While encryption is a key method for securing cloud data, it may not fully protect against legal access by foreign governments (El Makkaoui et al., 2015). Additionally, insider threats from employees of foreign cloud providers pose significant risks, emphasising the need for stringent security policies and careful selection of service providers.

Data sovereignty is challenging to achieve or safeguard when the data is stored in a foreign legal jurisdiction. Data Sovereignty refers to the concept that data is subject to the laws and governance structures within the nation where it is collected or processed, including that nation having authority, control and oversight over that data (Mitchell & Samlidis, 2022). The broader term "digital sovereignty" includes the policies and measures used to maintain a level of control and authority over digital assets belonging to a country and its citizens (Mitchell & Samlidis, 2022).

As a result of the difficulty of asserting Digital Sovereignty over foreign-hosted data, "data residency" – the actual location of data – is an important aspect of Cloud Computing (Mitchell & Samlidis, 2022). Many countries have imposed data residency regulations that require data and its associated computing infrastructure to be based within the host country's territory (Mitchell & Samlidis, 2022), with data privacy often being the cited reason for these

requirements (Millard, 2015).

For isolated nations utilising foreign cloud services, enforcing data sovereignty can run counter to their objectives when balanced against the need to access offshore digital infrastructure (Couture & Toupin, 2019). Enforcing digital sovereignty in such cases can inhibit the functioning of critical technologies for such nations (Mitchell & Samlidis, 2022). Data stored in overseas data centres may be subject to foreign laws, potentially conflicting with local regulations and leading to legal disputes (Couture & Toupin, 2019). For example, the case of *Microsoft Corp. v. United States* highlights the challenges of cross-border data access and the complexities involved in enforcing national laws on data stored abroad (Kirschenbaum, 2018). Legally, isolated nations are at a disadvantage when enacting policies to guarantee digital sovereignty, and are forced to make exceptions that in turn can expose data to breaches or other risks. For example, New Zealand's data sovereignty regulations had to consider the reality that the country had no Cloud data centres when the regulations were crafted. As a result, the regulations stated that, for data sovereignty purposes, New Zealand data could be stored in jurisdictions with laws similar to those of New Zealand (Digital Government New Zealand, 2024). This had the effect of limiting certain types of data (such as healthcare data) to Cloud data centres based in Australia, the UK, the US, Ireland, or Canada. In other cases, isolated nations are forced to exclude data and information provisions from their bilateral agreements to avoid jeopardising access to foreign Cloud data centres (Couture & Toupin, 2019). This places them at a significant legal disadvantage when attempting to enforce digital laws and regulations over that data.

The Economic costs of non-domestic data centres can be significant. Utilising non-domestic data centres carries with it a cost element that must be borne by the subscribing country (Cantu-Bazaldua, 2021). The subscribing country often incurs higher operational costs due to data transit fees and currency exchange rates (Cantu-Bazaldua, 2021; Hu et al., 2019). These

expenses can strain the limited financial resources of small or isolated countries, making digital services less affordable for their populations.

Reliance on foreign-based cloud services also presents challenges related to *job displacement* and *increased dependence on external technology providers*, potentially resulting in loss of local jobs and the erosion of domestic IT expertise (Charyyev et al., 2020). This shift could create or worsen a skills gap in the local workforce as the demand for local IT professionals decreases.

Chapter 3

Related Work

This work is focused on the challenges faced by small and isolated countries that rely on foreign data centres for their Internet services. The related work discussed in this Chapter investigates these challenges and the implications of this reliance for network performance, data sovereignty, and other factors. The Chapter is organised into two sections: the first section, (Section 3.1), discusses the performance implications of relying on foreign data centres for Cloud services, while the second section, (Section 3.2), reviews other related studies that have addressed the challenges of relying on foreign data centres for Cloud services.

3.1 Performance

As discussed in (Chapter 2), quality of Internet services plays a vital role in business operations and economic growth (Obren & Howell, 2014). With the increasing reliance on Cloud Computing, network performance factors such as latency, jitter, and packet loss have become critical in assessing service quality (European Telecommunications Standards Institute (ETSI), 2008). Small and isolated countries, which often depend on foreign-hosted Cloud services, sometimes face degraded performance due to geographic distance and suboptimal routing configurations (Geleji, 2011). In addition to performance, the selection of Cloud Service Providers (CSPs) is a complex optimisation prob-

lem that involves balancing cost, security, and performance (Hu et al., 2019). This is often compounded, in the case of small and isolated nations, by the lack of domestic Cloud data centres, which forces many governments and businesses to host digital assets abroad (Kumar et al., 2024). For those countries, the global Submarine Cable Network is a critical part of their Internet infrastructure, yet its vulnerability to natural disasters and geopolitical risks raises concerns about network resilience (Msongaleli et al., 2015). This section reviews research that demonstrates the influence of network performance, CSPs selection, and the threats to the SCN on system reliability, scalability, and overall user experience in small and isolated countries.

Internet quality and performance is a critical factor of business and economic growth. (Dillon & Vossen, 2015) established that the increased adoption of Cloud Services by businesses in countries around the world means that performance of the Internet is an important factor in promoting good economic performance. However, where such services are hosted in foreign data centres, the quality of the Internet service can be compromised by high latency and other factors. Some of the main reasons for adopting Cloud Services are cost savings, flexibility, and scalability (Dillon & Vossen, 2015). Where such scalability is compromised by high latencies, the benefits of Cloud Services can be eroded. These findings were supported by (Tongsuksai et al., 2023), whose work focused on Cloud Enterprise Resource Planning (ERP) systems in New Zealand, and found that the main reasons for adopting Cloud ERP systems include the desire for system reliability, data security, reduced time to implement, affordability, increased accessibility and scalability. The attractiveness of these features to businesses has led to the increased adoption of Cloud ERP systems in New Zealand (Tongsuksai et al., 2023). A significant hurdle to attaining these benefits is the *quality of the Internet service*, as established by (Dillon & Vossen, 2015). Small and isolated countries were found to be more commonly adversely affected by poor Internet service quality, as established by (Zaki et al., 2014). Such sub-optimal Internet access, which

includes high latency, also showed up in the difficulties of processing complex web pages when there are circuitous routing configurations and redirections involved, as is sometimes the case with small or isolated countries that do not have their own Cloud data centres. Further research by (Dang et al., 2021) supported the finding that the most impact on latency comes from geographical distance to the data centre rather than congestion, which would be the other reason This is relevant to the Internet quality experienced by small and isolated countries that rely on other jurisdictions for their Internet services, as distance is usually significant between the foreign-hosted data centres and the users in the small or isolated country. Their research also found that many Internet Service Providers (ISPs) have invested in "edge computing" by deploying compute servers close to their users to avoid the latency challenges posed by having data centres geographically distant from users (Dang et al., 2021). However, as discussed elsewhere in this chapter, this does not always work as an alternative to hosting such applications in local Cloud data centres.

The performance observed by users will be affected by the multiple parts of the infrastructure, such as broadband access. (Obren & Howell, 2014) tested the claim that investments in ultra-fast local broadband access unconditionally facilitates improvements in national economic performance, and found them to be untrue. The work established that the relationship between broadband access and economic performance is not straightforward, and that the quality of the Internet service at the "last mile" is a critical factor in determining the economic benefits that can be derived from broadband access (Obren & Howell, 2014). This in turn is affected by distance from the data centre, as established by (Dang et al., 2021), which also found that the "tyranny of distance" and its resultant latency challenges remain a critical blocker to the economic benefits that can be derived from broadband access (Obren & Howell, 2014). The general conclusion is still that good Internet Infrastructure is important for economic performance, even though there are other factors within that infrastructure that can affect the economic benefits that can be

derived from it.

Latency is a key factor in assessing Internet service quality. In recognition of the importance of good Internet performance, the European Telecommunications Standards Institute (ETSI) uses latency as one of the proxy indicators for assessing Internet service quality, alongside jitter and packet loss (European Telecommunications Standards Institute (ETSI), 2008). When working with latency-sensitive applications, it is important to have low latency, as established in the research carried out by (Charyyev et al., 2020). The work found that edge computing can help reduce latency and improve the performance of latency-sensitive applications, and that non-uniform server deployment and load balancing by an edge provider that takes latency into account can help improve the performance of latency-sensitive applications (Charyyev et al., 2020). However, this does not always work as an alternative to hosting such applications in local Cloud data centres. Work by (Maheshwari et al., 2018) presented an analysis of the scalability and performance of Edge Cloud systems designed to support latency-sensitive applications. The work found that core cloud-only systems actually outperform edge-only systems, making the case for investment in local Cloud data centres to avoid compromising the potentially better Cloud-only performance by having to deal with increased latency.

Performance engineering is a critical component of achieving good Internet quality, especially in the age of Cloud Computing. Early views of Cloud Computing saw it as potentially solving the challenges associated with engineering and managing large software systems, as established by (Murphy, 2011). Ironically, views at the time were that performance engineering would become redundant due to the ability to scale. However, (Murphy, 2011) argued that performance engineering would still be relevant, and that the challenges of performance engineering could not be wished away by 'cloud-washing' (Murphy, 2011) – given that Internet access will always be limited by physical infrastructure. To help with the performance engineering of Cloud-

hosted systems, the placement of data applications within Cloud infrastructure matters, as (Jia & Wang, 2022) established. The service components of data-intensive applications are commonly placed on edge or Cloud servers to minimise latency, but many such deployments ignore optimisation as a way of obtaining better performance. The work found that using an optimisation strategy can help achieve better outcomes when coupled with edge placement. The perception of performance metrics is important, particularly when it is by end users. (Lai et al., 2020) investigated the measurement and management approaches used to assess Internet performance, and found that the use of pre-configured websites such as ookla's "speedtest" service may miss out on important parameters such as jitter and packet loss, and could thus an unreliable indicator of Internet service quality (Speedtest by Ookla, 2025). This is despite such services being very popular with end users (Lai et al., 2020). An example of an ookla speedtest result is shown in Figure 3.1 below, showing latency and bandwidth, but without other measures like jitter and packet loss.

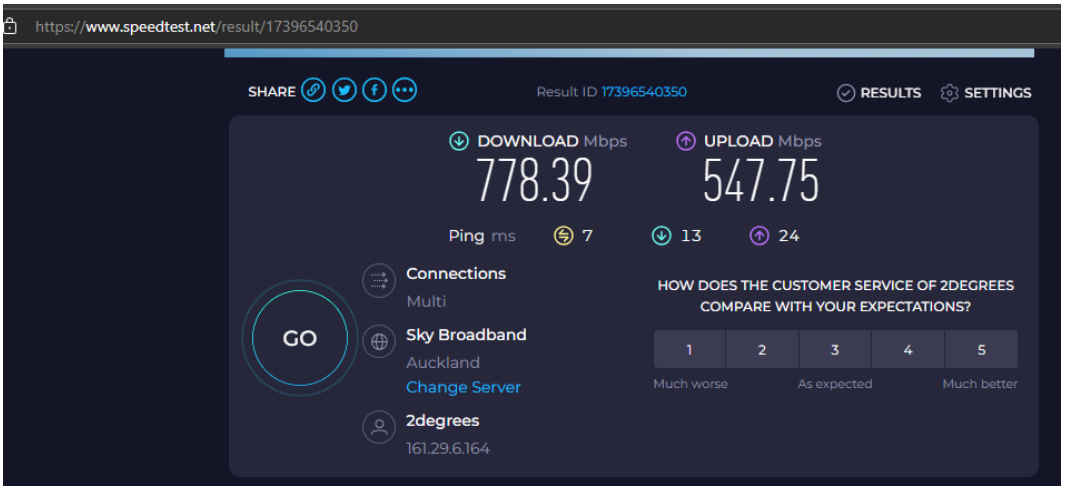

Figure 3.1: Sample Ookla Speedtest Result

(Speedtest by Ookla, 2025)

The existing choices of Cloud Service Providers can be a challenge when selecting where to host one's Internet services. (Hu et al., 2019) evaluated the challenges involved in selecting data centres from multiple Cloud Service Providers (CSPs) to reduce cost while maximising performance. The work found that the selection of data centres from multiple CSPs can be

a complex optimisation problem, and that the use of a genetic algorithm can help in selecting the best data centres to achieve the desired performance at the lowest cost. This selection needs to keep factors such as security and privacy in mind. (Bhajantri & Mujawar, 2019) explored the security challenges posed by Cloud Computing. They reviewed security issues at infrastructure, data, and Identity and Access Management (IAM) levels, and found that the security challenges posed by Cloud Computing are complex and multi-faceted. They proposed solutions for each of these security challenges, and found that the use of encryption, multi-factor authentication, and secure data transmission and storage can help mitigate the security challenges posed by Cloud Computing (Bhajantri & Mujawar, 2019).

The Submarine Cable Network (SCN) is a critical and concerning part of the Internet's infrastructure. Various proposals have been developed to make the SCN more robust in the face of natural and other risks, as discussed in (Chapter 2). (Msongaleli et al., 2015) conducted research into disaster-aware submarine fiber cable deployment. The work found that today's social and economic reliance on the Internet makes network survivability a critical issue, and that the deployment of submarine fiber cables should take this into account when selecting paths for the cables. They proposed an algorithm that can help with the decision-making process in selecting optimal cable routes (Msongaleli et al., 2015). The criticality of the SCN is made more apparent by the fact that much of the Internet is increasingly centralised in a few Cloud Service Providers, as established by (Moura et al., 2020). Work by (Moura et al., 2020) studied these concerns (around Internet centralisation), as well as the consolidation of traffic, users and infrastructure in the hands of a few market players. The work found that a large percentage of Internet traffic is concentrated in a few very large Cloud Providers, and assessed the impacts of that centralisation on the Internet's performance and resilience (Moura et al., 2020). In this context, the SCN acts as a point of failure for the Internet, and even more so for small and isolated countries that rely on one or two SCN

cables for their Internet access.

Network delays and packet loss can have a significant negative impact on the experience of Internet users. (Chen et al., 2009) analysed the impact of network performance on the satisfaction of game-playing users on the Internet. Their research established that player intolerance to network delay and network loss is widespread within the gaming community. Their findings have relevance for the general experience of Internet users, as the same factors that affect game-playing users can also affect other Internet users. They recommended that prioritising server processing based on network conditions, and employing dejitter buffers to reduce network delays and minimise packet loss can be effective in improving the satisfaction of game-playing users on the Internet (Chen et al., 2009). This experience was also observed for Internet users whose main application was web-page loading. (Schlinker et al., 2019) observed that beyond speeds of about 8Mbps, latency is the main bottleneck for page load times and access to other Internet-hosted resources, and went on to quantify performance as seen from the edge of a large Internet service provider, Facebook (Schlinker et al., 2019).

Lack of domestic data centres often forces the governments of small and isolated countries to host their digital assets overseas. In New Zealand, (Kumar et al., 2024) found that 40 percent of government Universal Resource Locators (URLs) are served from Australia. The lack of major cloud providers data centres in New Zealand has meant that many Software as a Service (SaaS) applications used in New Zealand are served from Australia and the United States. This has performance, security, and cost implications for the customers of these services (Kumar et al., 2024). In addition, making informed choices between Cloud Service Providers can be a challenge, and can frequently require the use of sophisticated tools to make the best choice (Palumbo et al., 2021). Work by (Palumbo et al., 2021) involved carrying out a comparative analysis of two Cloud Service Providers (Microsoft Azure and AWS). Using a detailed latency comparison, they developed a tool

that can be used to select the most suitable Cloud Service based on latency performance and calculated cost of access.

3.2 Other Factors

Data Sovereignty and Privacy are ever-present concerns for countries that rely on foreign-hosted Internet services. (Mitchell & Samlidis, 2022) investigated the implications of using foreign data facilities on Data Sovereignty and Privacy, with a focus on Australia. The work found that governments and public sector players in Australia and elsewhere are concerned about the implications of using foreign data facilities for their Internet services, and are considering the implications of data sovereignty and privacy in their procurement decisions (Mitchell & Samlidis, 2022). The work also established that Australia has introduced digital sovereignty measures and requirements to protect government technology systems and data. These measures have had the effect of increasing the cost of using foreign data facilities for government technology systems and data (Mitchell & Samlidis, 2022), as well as the administrative overhead involved in such uses. Where Cloud services such as SaaS are not available within Australia, significant security mitigations are required to ensure that data sovereignty and privacy are maintained.

The manner in which indigenous peoples' data is handled is an important component of data sovereignty. In New Zealand, for example, Maori Data Sovereignty is an important consideration for all data hosted in foreign data centres. (Sharma et al., 2024) made the point that people should be able to govern data about themselves and their ways of life, and that the data should be used in ways that are consistent with their values and aspirations. However, this is not always possible to enforce when such data is stored in offshore data centres, as is the case for many small and isolated countries (Sharma et al., 2024). The researchers proposed a trustless approach for indigenous geospatial data sovereignty in the Cloud by furnishing security

functions at the Web Browser level, with geomasking or other forms of data masking, and encryption of data. This approach is based on the observation that there is a generic lack of trust in the Cloud, and that this lack of trust is particularly acute for indigenous peoples (Sharma et al., 2024). This mistrust results in a need for more clarity in the discussions about data sovereignty and localisation, as established by (Millard, 2015). The work found that the debate is often characterised by a lack of clarity, and that the term "data sovereignty" is often used to mean different things by different people. The work also found that the debate is often characterised by a lack of trust in the ability of foreign data centres to protect data, and that this mistrust is often based on a lack of transparency and accountability in the operations of foreign data centres.

Big Data has made data sovereignty and privacy even more complex – and important. The growth in the use of Big Data services has significant implications for data sovereignty and privacy (Cherrington et al., 2020). According to that study, advances in Big Data analytics often are made without regard to indigenous digital rights, and that there is a responsibility on the part of Big Data service providers to build tools that help enforce respect for the digital rights of indigenous peoples. Small and isolated countries are unlikely to have a domestic Big Data industry, and are thus likely to rely on foreign Big Data service providers. This carries with it the risk of compromising data sovereignty and privacy, as the concerns of such small countries are seldom included in discussions and decisions on the matters (Cherrington et al., 2020). These findings were supported by (Bowen & Hinze, 2022) and (Sharma et al., 2024), both of whom addressed the cultural considerations and data ownership rights of data owners and users. They argued that people should be able to govern data about themselves, their territories and ways of life, and that security functions needed to be provided in digital platforms to facilitate indigenous data sovereignty.

Outdated laws and regulations can pose challenges to the use of Cloud Computing. Work by (Mutkoski, 2015) established that many of

today's laws and regulations that apply to Cloud Computing, as a subset of digital systems, were developed *before* the advent of Cloud Computing, and that they are not well-suited to the challenges posed by Cloud Computing. This is because many such laws were inherited from previous eras of computing, and were not designed with the unique challenges of Cloud Computing in mind. The work explored some of the legal and regulatory challenges posed by Cloud Computing, and found that there is a need for new laws and regulations that are better-suited to the corresponding challenges (Mutkoski, 2015). Revamping the laws and regulations governing Cloud Computing can help address some of these issues, and can ensure that Cloud Computing is used in a way that is consistent with the values and aspirations of the people who use it. However, this is expensive, and can be a significant barrier to the adoption of Cloud Computing by small and isolated countries when they have to weigh the costs of their own legal compliance against the benefits of using Cloud Computing.

For small countries, an additional challenge is "long-arm jurisdiction", which is the legal ability of a country to enforce its laws on data stored in foreign data centres. (Kushwaha et al., 2020) examined the ways in which data stored in foreign data centres is affected by long-arm jurisdiction. In particular, legal regulations in the United States and the EU were found to have far-reaching implications for data stored within their jurisdictions. The work found that the use of long-arm jurisdiction to access data stored in foreign data centres can have implications for data sovereignty, and that there is a need to balance data sovereignty with the needs for law enforcement and national security (Kushwaha et al., 2020). Small and isolated countries are particularly vulnerable to long-arm jurisdiction, as they lack the resources to enforce their own laws on data stored in foreign data centres.

These and related concerns result in challenges for small and isolated countries that rely on foreign data centres for their Internet services. (Pohle & Thiel, 2020) investigated the challenges to data sovereignty posed by the use

of Cloud Services and foreign data centres. The work found that sovereignty is re-emerging as a key category for the governance of data, and that there is a need for new approaches to data governance that take into account the unique environment presented by Cloud Services and foreign data centres (Pohle & Thiel, 2020).

Chapter 4

Methodology: Performance Tests and Cloud Services Access Factors

4.1 Introduction

This chapter outlines the methodology used to quantify the performance of Cloud services accessed from New Zealand, focusing on latency, jitter, and packet loss. Measurements were conducted using multiple vantage points, including the network of Mercury Energy Ltd, RIPE Atlas probes in Australia, and a virtual machine in Azure's Australia region. The primary aim is to analyse network performance for Cloud services hosted outside New Zealand, identifying any significant delays or disruptions. Additionally, this chapter presents the key research questions guiding the study and details the measurement techniques employed to evaluate Cloud access performance from an isolated nation's perspective.

As discussed in Chapter 2, Cloud computing has enabled isolated countries to access advanced digital services without requiring substantial infrastructure investments (Kshetri, 2010). However, despite this benefit, performance issues such as latency, jitter, and packet loss can significantly impact the usability of Cloud services from these locations (European Telecommunications Standards Institute (ETSI), 2008). The long physical distances between users and

Cloud data centers, as well as the quality of intermediate Internet connections, contribute to these performance degradations.

The aim of the work carried out in this chapter is to quantify latency, jitter, and packet loss as a proxy for the performance of Internet services and also the performance of Cloud computing services for isolated countries, with New Zealand as a case study. The work will highlight network performance as a function of latency, jitter, and packet loss, and identify low or unsatisfactory performance as observed during the data collection. The performance data used in this analysis was collected by carrying out measurements from the Mercury Energy Ltd (a New Zealand-based energy company and Internet Service Provider) network starting from November 15 2024 to December 15, 2024. Additional data was collected using RIPE Atlas probes located in Australia, and from a virtual machine in the Azure Cloud located in Australia.

The working questions used in the performance measurements were:

- What is the observed latency when accessing foreign-hosted Cloud services from New Zealand? The Cloud services targeted for this question were AWS in Australia, Azure in Australia, and Azure in the USA. The question provided New Zealand-specific latency observations for services hosted by the named Cloud providers.

- What are the observed characteristics of jitter and packet loss when accessing computing resources located in foreign-hosted Cloud services?

4.2 Metrics Selection

The approach taken to measure the performance of foreign-hosted Cloud services was based on the position that isolated countries do not always receive reliably high-performance access to foreign-hosted Cloud services. For New Zealand, this is particularly true when accessing Cloud services because any access to public Cloud in New Zealand at the time of writing meant that the

services were hosted in Australia or elsewhere outside of New Zealand (Sorenson, 2024).

Three widely-used metrics were selected to be measured as indicators of performance: latency, jitter, and packet loss (European Telecommunications Standards Institute (ETSI), 2008). Some of the poor performance and experience is likely due to the high end-to-end delays (latency) caused by the long distances between the isolated country and the foreign-hosted Cloud services. Measuring such delays provides important information about the delays experienced by users in such countries. Packet loss and jitter are also important indicators of the quality of the Internet service, as they can cause retransmissions and thus increase the time taken to load web pages and other Internet-hosted resources (European Telecommunications Standards Institute (ETSI), 2008).

It should be noted, however, that the actual performance of Cloud Services would be affected by a range of factors, including the number of network hops, the quality of the network connections, and the efficiency of the data centres themselves. In addition, typical Internet transactions do not involve a single round trip, but multiple interactions between the user endpoint and the and the data centre endpoint. As a result, the metrics discussed here are indicative of what happens in single RTTs, and may not fully capture the performance of Cloud Services in real-world scenarios where Web browsers carry out complex interactions and return multiple sets of data with each request.

In such real-world cases, the effects observed in this study would be multiplied many times, leading to a significant impact on the user experience. The results of this study are therefore a starting point for understanding the challenges faced by isolated countries in using foreign-hosted Cloud Services, and provide a basis for further research and analysis.

Jitter was calculated based on the formula below (Shreya & Saini, 2023):

$$\text{Jitter (ms)} = \frac{\sum_{i=1}^{n-1} |T_{i+1} - T_i|}{n-1}$$

where

- T_i is the time taken for the ith packet to reach the destination
- n is the total number of packets sent

Packet loss was calculated using the following formula (Kodali et al., 2019):

$$\text{Packet Loss (\%)} = \left(\frac{\text{Total Packets Sent} - \text{Total Packets Received}}{\text{Total Packets Sent}} \right) \times 100$$

where

- Total Packets Sent is the number of packets sent from the source
- Total Packets Received is the number of packets successfully received at the destination

4.3 Measurements Design

Measuring Internet performance can be approached in a number of ways, including active and passive measurements, and using a variety of tools and platforms (Sermpezis et al., 2023). Various Internet platforms have deployed measurement tools that can be used to observe the performance of the Internet. RIPE Atlas is an open platform that allows its users to carry out various measurement activities on the Internet, including traceroute, ping, DNS, SSL, and related measurements (Bajpai et al., 2015). RIPE Atlas has a widely distributed network of probes that are employed to carry out a wide variety of Internet-related measurements, although there are some inbuilt biases towards certain regions and countries – and urban areas (Sermpezis et al., 2023).

In order to assess the performance of foreign-hosted Cloud resources as accessed from New Zealand, a measurement campaign was carried out over a period of 4 weeks, assessing selected metrics that are indicators of network performance and quality. The measurements were conducted from three locations:

- The network of Mercury Energy Ltd, a New Zealand-based ISP.
- RIPE Atlas probes located in Australia, where the targeted Cloud Services are located.
- A virtual machine in the Azure Cloud located in Australia.

The measurements were based on three vantage points. The first one was a set of probes part of the RIPE Atlas infrastructure, used to measure latency from New Zealand to commonly-used Cloud platforms hosted outside New Zealand. The second was a virtual machine set up in a cloud service provider (Azure) in Australia to compare the resultant metrics against those observed using RIPE Atlas. The third was the network of Mercury Energy Ltd.

The Australia-based virtual machine was located in the "Australia East" region of the Azure Cloud service (Microsoft, 2025a). The US Cloud services were located in the "West US" region of the Azure Cloud service (Microsoft, 2025b).

For each metric, the measurements were carried out successively from the selected platform 5 times per day, for 4 weeks, from November 15, 2024 to December 15, 2024. The times when the measurements were carried out differed, to ensure that the measurements were not biased towards any particular time of day. As a result, some measurements were carried out during peak hours, while others were carried out during off-peak hours. Not all Cloud Provider endpoints could be reached all the time – where this was the case, the measurements were repeated until the total number of measurements reached 10,000. The number of measurements was set at 10,000 to have a large enough sample size that would ensure that the results were statistically significant and representative of the performance of the Cloud services. All measurement results were collated and analysed to determine the average latency, jitter, and packet loss for each Cloud service for every day of the measurement period. The daily averages were then used to calculate the overall average for the entire measurement period for each metric per Cloud service.

- Traceroute measurements were carried out from the Mercury Energy Ltd network in New Zealand to the IP addresses of selected AUS Cloud Services in Australia to compare the numbers of hops and the time taken to traverse them to reach the respective destinations.

- Traceroute measurements were carried out from the Mercury Energy Ltd network to the IP addresses of selected Cloud services in the United States.

- Traceroute measurements were carried out from an Australia-based virtual machine in the Azure Cloud to the IP addresses of the selected AUS Cloud Services in Australia.

- Ping measurements were carried out in the same way as the Traceroute measurements above:

  - One set of measurements was carried out from the Mercury Energy Ltd network in New Zealand to the IP addresses of the AUS Cloud Services in Australia.

  - Another set of measurements was carried out from the Mercury Energy Ltd network to the IP addresses of the Cloud services in the United States.

  - The final set of measurements was carried out from an Australia-based virtual machine in the Azure Cloud to the IP addresses of the AUS Cloud Services in Australia.

- Jitter and Packet Loss measurements and calculations were carried out from the Mercury Energy Ltd network in New Zealand to the IP addresses of the AUS Cloud Services in Australia and the United States, as well as from an Australia-based virtual machine to Australian Cloud Services (Azure Cloud).

These measurements are summarised in Tables 4.1 and 4.2.

Measurement Type	Source Location	Target Location	Description
Traceroute	MercuryNZ	AUS Cloud Services	From NZ to Aus
Traceroute	MercuryNZ	US Cloud Services	From NZ to USA
Traceroute	Azure VM (Aus)	AUS Cloud Services	From Aus to Aus
Ping	MercuryNZ	AUS Cloud Services	From NZ to Aus
Ping	MercuryNZ	US Cloud Services	From NZ to USA
Ping	Azure VM (Aus)	AUS Cloud Services	From Aus to Aus
Jitter & Packet Loss	MercuryNZ	AUS Cloud Services	From NZ to Aus
Jitter & Packet Loss	MercuryNZ	US Cloud Services	From NZ to USA
Jitter & Packet Loss	Azure VM (Aus)	AUS Cloud Services	From Aus to Aus

Table 4.1: Measurement Types and Locations

Key: NZ = 'New Zealand'; Aus = 'Australia'; US = 'United States of America'

Measurement Details	Description
Measurement Frequency	5 random times per day, for 4 weeks
Total Measurements	10,000
Measurement Repetition	Repeated until 10,000 measurements reached
Measurement Platforms	Mercury Energy Ltd network, RIPE Atlas probes, Azure VM
Measurement Regions	Australia East (Azure), West US (Azure)

Table 4.2: Measurement Details

4.4 Non-Technical Factors Review

In addition to the technical factors, the performance of foreign-hosted Cloud services as accessed from remote countries is also influenced by, among other non-technical factors:

- Availability and resilience of undersea fiber cables given geopolitical and other factors (Astier & Kirby, 2024)
- The legal and regulatory environment affecting such access (Pohle & Thiel, 2020)

A review was undertaken of these factors and how they affect access to Cloud services from small and isolated countries, with a focus on New Zealand.

Undersea Fiber Cables form the backbone of international Internet connectivity, as discussed in Chapter 2, and the availability and resilience of these cables are critical to the performance of Internet services in isolated countries (Msongaleli et al., 2015). For example, New Zealand is connected to the rest of the world by a number of undersea fiber cables, including the Southern Cross Cable Network, the Tasman Global Access cable, and the Hawaiki cable (Submarine Networks Company Ltd, 2025). Disruption to these cables – whether accidental, deliberate, or due to natural events like earthquakes or volcanic eruptions – can severely impair access to Cloud Services hosted outside New Zealand. For small and isolated countries, the risk of prolonged outages as a result of such events is made worse by the lack of alternative routes for Internet traffic to take (Msongaleli et al., 2015). This makes their dependence on foreign-hosted Cloud Services a risky position – particularly in regions of the world with significant natural disaster prevalence or with heightened geopolitical tensions. Pakistan, for example, depends significantly on foreign-hosted Cloud Services, and has recently experienced severely disrupted business operations following several major submarine cable faults (Opalinski et al., 2024). This, and the experiences of Baltic countries that are caught up in geopolitical tensions between NATO and Russia (Pirenne et al., 2024), has led to concerns about the security of undersea fiber cables around the world. In the Baltic region, several recent cable cuts have been blamed on foreign actors, principally Russia and China (Aggarwal, 2025).

The Legal and Regulatory Environment also plays a significant role in determining the availability and performance of foreign-hosted Cloud Services as accessed from isolated countries. The legal and regulatory environment in the affected country can affect the performance of Cloud Services in a number of ways, including:

- Data sovereignty laws that require data to be stored within the country's borders (Jansen et al., 2023).

- Data protection laws that require data to be stored in a particular way or to be encrypted (Sharma et al., 2024).
- Data transfer laws that restrict the movement of data across borders (Pohle & Thiel, 2020).

For example, New Zealand has data protection laws that require various types of citizens' data to be stored in particular ways, and data transfer laws that restrict the movement of such data across borders (Cherrington et al., 2020). These laws also have implications for the way Maori data is stored and accessed, which in turn narrows the range of Cloud Services that can be used to store and process such data (Cherrington et al., 2020). As defined by (Te Mana Raraunga, 2025), New Zealand's Māori Data Sovereignty Principles require that Māori data is stored in a way that respects Māori rights and interests, and that Māori have control, authority and jurisdiction over how their data is used. Ensuring these requirements are met involves making provisions for access, ensuring disaggregation, providing for accountability, restrictions, and recorded consent (Te Mana Raraunga, 2025) Such measures have cost implications, as they require Cloud Service Providers to provide technical capabilities above and beyond their normal service offers. This can can increase the cost of Cloud Services for users in the affected country (Cherrington et al., 2020).

New Zealand is located in a seismo-volcanic zone. This makes the country significantly exposed to earthquakes and volcanic eruptions, which can disrupt undersea fiber cables and other Internet infrastructure (Submarine Networks Company Ltd, 2025). The experience of Tonga in 2022, when the Hunga Tonga-Hunga Ha'apai volcano erupted and disrupted Internet services for several days, provides learnings for New Zealand in the need to build resilience into its Internet infrastructure (Wang et al., 2023). A review was undertaken of the risks that such events could pose for New Zealand, and the measures that could be taken to mitigate them, and they will be presented in the next chapter.

Chapter 5

Results and Discussion

5.1 Performance Tests Results

1. Time Taken To Traverse Network Paths Using Traceroute:

The average times for the traceroute measurements are shown in Figure 5.1.

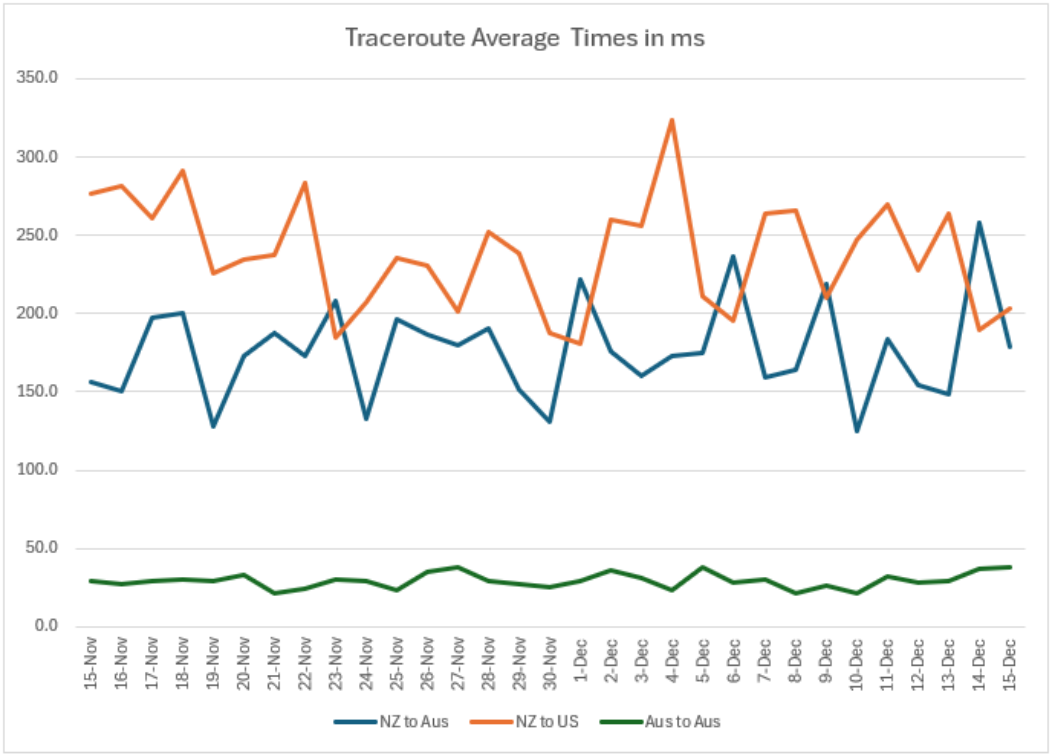

Figure 5.1: Traceroute Measurement Results

The network paths taken by data packets from New Zealand to the US West Coast were significantly longer than those taken to Australia, and much

longer than those taken within Australia. This was reflected in the traceroute measurements, whose results showed that the average number of hops and the time taken to traverse them from New Zealand to the US West Coast were significantly higher than the same metrics between New Zealand and Australia, and much higher than within-Australia measurements. This trend illustrates the significant impact of geographical distance on the time it takes data to traverse network paths as well as, potentially, the number of hops involved in the path. A review of the data indicates there could be other factors at play, including congestion, routing policies, and peering agreements. The general trend supports the expectation that NZ-to-US routes will show the highest latency in this study, some anomalies do appear in the dataset. For example, on December 6th, 2024, the traceroute from New Zealand to the US West Coast showed a lower average latency than the same metric between New Zealand and Australia, before falling back to the expected higher latency on December 7th, 2024. This suggests temporary network congestion or suboptimal routing at the time of the spike. These variation in latency across different days may also indicate dynamic routing adjustments made by ISPs or changes in traffic load during peak hours - a practice that is common in the industry (BITAG, 2022). The observation of relatively stable AUS-to-AUS latencies reinforces the importance of regional infrastructure investment, as users in Australia consistently experience lower delays when accessing locally hosted content compared to users in NZ accessing foreign-hosted services. This is consistent with the findings of (Dang et al., 2021) that one of the most significant impact on latency comes from geographical distance to the data centre.

The implications of these findings are critical for Cloud service accessibility and digital infrastructure planning in small and isolated countries. The high latencies to the US highlight a major challenge for businesses and governmental agencies that rely on US-based Cloud providers, reinforcing arguments for establishing more regional Cloud data centers in NZ and in other geographically

isolated regions. While Australia serves as a partial intermediary with moderately lower latencies, it is still not an ideal substitute for local hosting when low-latency performance is essential. The consistently low AUS-to-AUS latencies provide evidence supporting regional data centre placement as a means of mitigating performance degradation caused by transoceanic routing. Additionally, given the increasing reliance on Cloud-based applications and Content Delivery Networks (CDNs) (Yang et al., 2023), improving the Cloud and network infrastructure setups of isolated countries (including via direct peering, undersea cable investments, or strategic partnerships with Cloud providers) can significantly enhance the performance of Cloud Services and the resultant user experience for subscribers of those services. The results above also imply indicate that other mechanisms of bringing Cloud Services closer to the users in isolated countries - such as edge computing and caching to mitigate long-haul latencies - can improve the performance of Cloud applications and services that need real-time responsiveness, such as video conferencing, online gaming, and financial services (Ray et al., 2022)[1].

2. Round-Trip Latency Using Ping:

The ping results showed that the average latency from New Zealand to the US West Coast was significantly higher than both the same metrics between New Zealand and Australia, and much higher than within-Australia measurements. Average ping times from New Zealand to Australia ranged within the 30-40ms band, while the same metric from New Zealand to the US West Coast was in the 170-180ms band. The average times for the ping measurements are shown in Figure 5.2.

[1]It should be noted that traceroute times to a given host will generally be longer than ping times to the same host, as traceroute involves sending multiple packets to each hop along the route, while ping typically only sends one packet to the destination (GeeksforGeeks, 2024). Ping operates at a more basic level than traceroute, and only checks if the destination host is reachable. Traceroute seeks to trace every host along the network path, making it take longer than ping, even for the same target host (GeeksforGeeks, 2024).

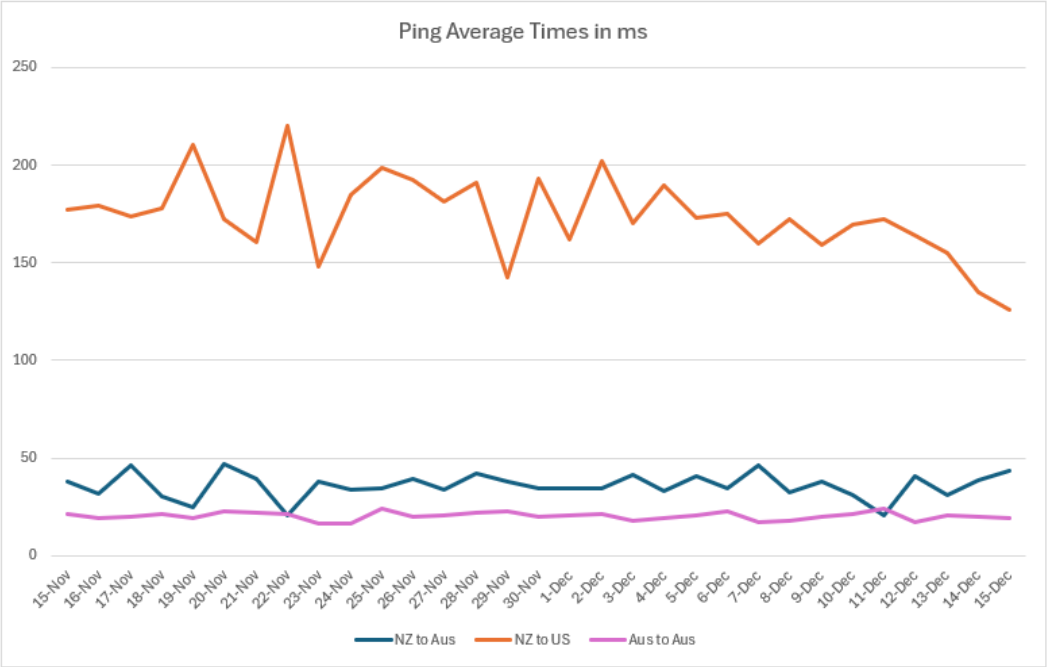

Figure 5.2: Ping Measurement Results

From the collected data, the average round-trip-times times computed were as follows:

$$\text{Average ping time (NZ to Australia)} = 35.891 \text{ ms}$$

$$\text{Average ping time (NZ to USA)} = 173.877 \text{ ms}$$

$$\text{Average ping time (Australia to Australia)} = 20.267 \text{ ms}$$

To determine how much faster round-trip-times were from NZ compared to Australia and the USA:

$$\text{NZ vs. Australia} = 35.891 - 20.267 = 15.624 \text{ ms}$$

$$\text{NZ vs. USA} = 173.877 - 35.891 = 137.986 \text{ ms}$$

Thus, on average, ping times from New Zealand were:

- **15.324 ms faster** than those to Australia.
- **137.986 ms faster** than those to the United States.

The ping latency results illustrate the Internet performance and accessibility of Cloud services from New Zealand to the US and Australia. The observed latencies between NZ and AUS are generally within the 30-50 ms range, whereas NZ-to-US latencies are significantly higher, often exceeding 150 ms, with peaks above 200 ms. The AUS-to-AUS latencies remain consistently low, averaging around 19-22 ms, emphasising the importance of having Cloud Data Centres in close proximity to the end users. This is consistent with the findings of (Dang et al., 2021)that the geographical distance between the user and the data centre is a key factor in determining latency. The relatively stable AUS-to-AUS latencies provide further evidence that Cloud Data Centres close to the end users can significantly improve the performance of Cloud Services and applications. In normal Internet usage, the impact of high latency would be felt the most in applications that need real-time data processing, such as online gaming, video conferencing, remote work environments, and VoIP calls (Chen et al., 2009). As a result, business users in remote and isolated countries who depend on foreign-hosted Cloud Services would experience better services if Cloud Data Centres were located closer to them, or if mitigating measures were put in place to reduce latency. Mitigating measures for high latency would include the use of Content Delivery Networks (CDNs) that cache data closer to the end users (Yang et al., 2023), and the use of edge computing to bring compute resources closer to the users (Dang et al., 2021), (Maheshwari et al., 2018). However, these measures would require significant investment in infrastructure, which may not be feasible for small and isolated countries. In addition, the use of CDNs may not be effective for dynamic content - such as data used in Cloud applications like Software as a Service - which would still need to be fetched from the original data centre. For these tasks, therefore, the inherent delay caused by geographical distance between the user and the data centre are challenging to overcome without local Data Centre infrastructure.

This findings also have implications for Cloud computing planning and in-

frastructure investments in isolated countries. The consistently higher latency to the US illustrates the challenges of hosting critical digital services in offshore data centres, which potentially degrades user experiences for businesses reliant on US-based Cloud platforms. The lower latencies to Australia suggest that it could serve as a partial remedy for New Zealand, but is not a perfect solution given the much lower latencies observed in AUS-to-AUS measurements. The variability in measurement results once more highlights the dynamic nature of Internet routing and the need for robust infrastructure planning and investments in additional undersea cables to ensure consistent performance for Cloud services.

3. Network Stability Observation Using Jitter:

Jitter is the variation in the delay of received packets, and is a measure of the stability of the network connection (Shreya & Saini, 2023). Jitter is a significant challenge for users dependent on foreign-hosted Cloud Services, as it can cause data packets to arrive out of order (European Telecommunications Standards Institute (ETSI), 2008), leading to data loss and the need for retransmissions (Zhao et al., 2024). Applications that require a steady data flow to maintain quality are negatively affected by high jitter, as inconsistent packet delivery leads to degradation in services - such as distorted video and audio playback (Shreya & Saini, 2023). Because of this, even small fluctuations in jitter can affect user experiences significantly (Shreya & Saini, 2023). The average values for the jitter measurements are shown in Figure 5.3.

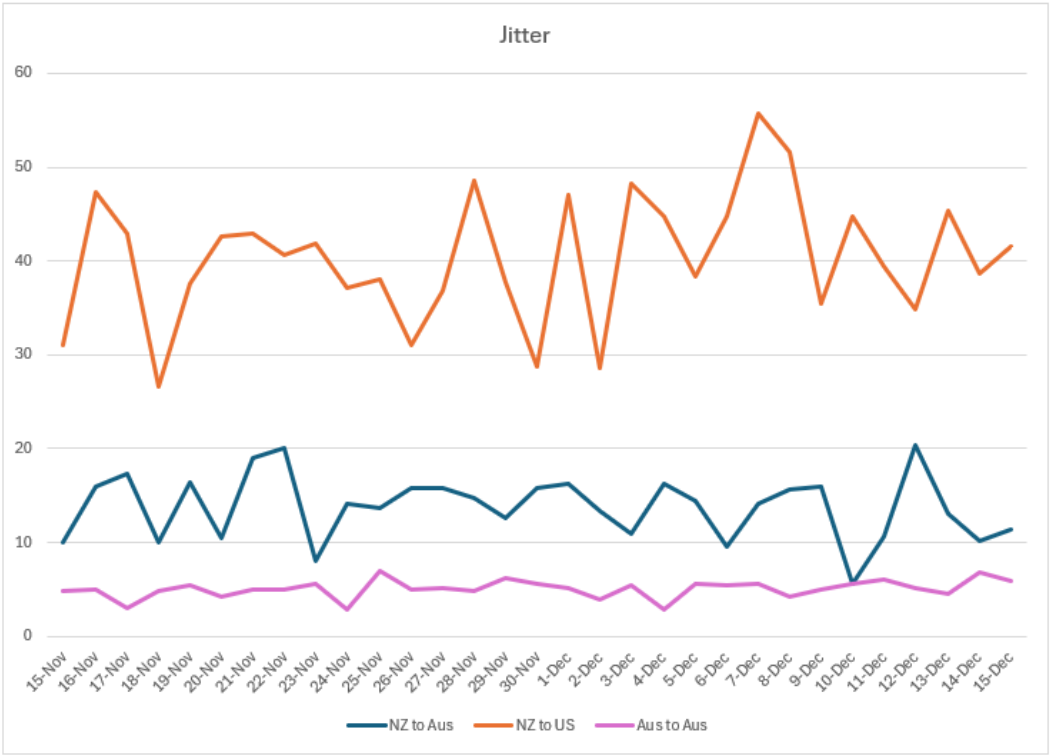

Figure 5.3: Jitter Measurement Results

The measurement results show that NZ-to-AUS jitter generally remained low during the observation period, averaging around 10–20 ms, while NZ-to-US jitter fluctuated more and was much higher. AUS-to-AUS jitter remained the lowest in the dataset, typically below 6 ms, indicating the importance of having users located close to their Cloud Data Centres in minimising Internet performance instability. Further, the higher jitter levels to the US provided more evidence that longer physical distances and complex routing paths make packet delay worse, leading to more unstable network connections. Isolated countries that rely on foreign-hosted Cloud Services are thus more likely to experience higher jitter levels due to the longer physical distances and complex routing paths involved in data transmission. This in turn means higher degradation of network performance and more challenges in ensuring reliable Cloud services for users. This is consistent with the findings of (Lai et al., 2020) that jitter is a key indicator of Internet service quality. Distance is not the only factor in the levels of jitter observed: it may also be a result of inconsistent routing paths and congestion at intermediate nodes (Geleji, 2011).

Mitigating measures for high jitter may include the use of Quality of Service (QoS) mechanisms to prioritise real-time traffic, and the use of jitter buffers to smooth out the variations in packet delivery (Zhao et al., 2024). A less efficient (but more straightforward) solution would be to increase or even overprovision the bandwidth of the network connection, which would allow more data to be transmitted at once, reducing the likelihood of congestion and jitter (Zhao et al., 2024). However, all of these measures involve additional costs and added complexity, and would thus be less accessible to government entities in small and isolated countries. They also do not resolve the underlying issue of geographical distance between the user and the Cloud Data Centre, which is the root cause of high jitter.

4. Network Reliability Measurement Using Packet Loss:

Packet Loss is the percentage of data packets that are lost during transmission, and is a measure of the reliability of the network connection (European Telecommunications Standards Institute (ETSI), 2008). The average values for the packet loss measurements are shown in Figure 5.4.

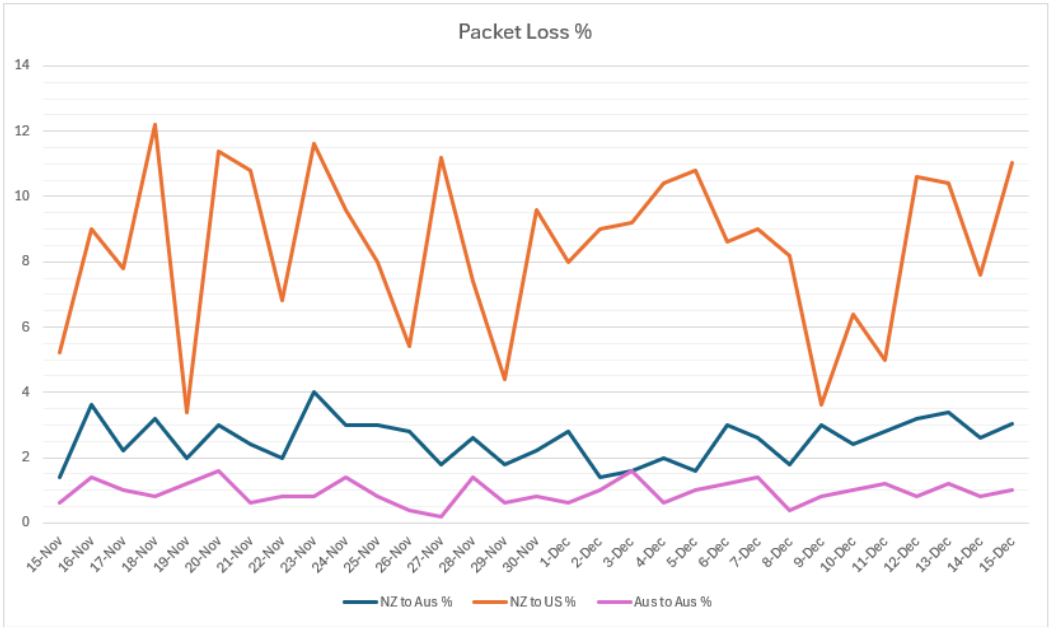

Figure 5.4: Packet Loss Measurement Results

Packet loss is an indicator of network congestion, possible routing inefficiencies, and/or network infrastructure limitations (Smith et al., 2016). The

results show a clear correlation between packet loss rate and geographical distance, with NZ-to-AUS packet loss typically ranging between 1.4% and 3.6%, while NZ-to-US experienced significantly higher loss rates, often exceeding 10% In comparison, AUS-to-AUS packet loss remains consistently below 2%, showing the advantage of having regional data centres and efficient domestic routing.

The results also showed a pattern of daily fluctuations in packet loss, indicative of sporadic congestion or rerouting affecting the network connections. Where packet loss spiked frequently, this may be an indicator of network instability, and could lead to service degradation for users reliant on foreign-hosted Cloud Services. This pattern was observed in the NZ-to-US packet loss measurements, which was likely due to the persistent challenges of maintaining reliable connectivity over long distances and complex routing paths. The much lower AUS-to-AUS packet loss rates indicate that closer proximity to Data Centres, lower network congestion, and optimised routing contribute to more reliable data transmission. The observed variations in NZ-to-US packet loss also suggest that network conditions are not uniform, with different days experiencing different loss rates due to variations in congestion or rerouting of traffic.

The implications of these findings are important for applications that require reliable data transmission such as file transfers, financial transactions and healthcare systems, all of which are quite intolerant of packet loss (Kodali et al., 2019). Such packet loss could lead to errors in data and delays caused by retransmission. The relatively high NZ-to-US packet loss rates raise concerns about the reliability of US-hosted Cloud services for businesses and institutions in isolated countries reliant on foreign Data Centres. That is because these levels of packet loss can severely impact the quality of real-time application performance. Where real-time decision-making (such as is the case with stock trading platforms or emergency response systems) is required, such packet loss could lead to significant financial or even human costs. Packet loss is an added

cost on the network (Ray et al., 2022), as lost packets must be retransmitted, leading to increased bandwidth usage and potential delays. For small and isolated countries, these additional costs can increase the challenges of using foreign-hosted Cloud Services.

5.2 Beyond Performance: Broader Challenges for Isolated Countries

The challenges of latency, jitter, and packet loss are just some of the technical hurdles faced by isolated nations relying on foreign-hosted cloud services. These performance issues are compounded by a range of broader risks that can threaten digital resilience and economic viability.

Security, Legal and Related Risks. Reliance on foreign-hosted Cloud Services increases vulnerability to cyber-attacks and data breaches (El Makkaoui et al., 2015). Sensitive data transmitted across international networks or stored in foreign jurisdictions is exposed to potential interception (Bhatta, 2023), with various actors having the motivation to invest in significant cyber-attack capabilities (Susantha et al., 2023). Further, the presence of pervasive insider threats in foreign data centres can compromise data integrity and confidentiality (Susantha et al., 2023).

Lack of local data storage options reduces national control over critical information (Pohle & Thiel, 2020), complicating the ability of such countries to assert control over their own data. Governments and businesses in isolated countries must often entrust their data to providers located in regions with differing legal and regulatory standards, raising concerns about data sovereignty (Couture & Toupin, 2019).

Significant security concerns arise from the using foreign-hosted Cloud Services. These include (Bhajantri & Mujawar, 2019):

- Data safety and privacy: Data stored in foreign data centres may be subject to different legal standards, increasing the risk of data breaches and unauthorised access.
- Non-compliance with local regulations: Data stored in foreign data centres may not comply with local data protection laws, leading to legal and regulatory risks.
- Loss of control: Data stored in foreign data centres may be subject to foreign laws and regulations, reducing national control over critical information, and potentially resulting in data leaks or related unauthorised access.
- Disaster recovery: Data stored in foreign data centres may be at risk in the event of natural disasters or political instability.

These challenges must be addressed through a combination of technical measures, such as encryption and access controls, and legal and regulatory frameworks that protect data sovereignty and privacy (Bhajantri & Mujawar, 2019). However, such mitigation invariably involves additional costs and complexity, which can be prohibitive for small and isolated countries, and further complicate their use of foreign-hosted Cloud Services.

Data Security in Offshore Data Centres can be challenging to ascertain and therefore to validate. When data is stored in a data centre, the general architecture abstracts the physical storage from the user, and the data is stored in a distributed manner across multiple servers (Zhang et al., 2020). The abstraction layer includes virtual servers and other virtual infrastructure, creating a three-layered framework that means the subscriber / end user is not directly aware of the physical location of their data (Zhang et al., 2020). This three-layered structure is shown in the diagram below (Zhang et al., 2020) (p.2):

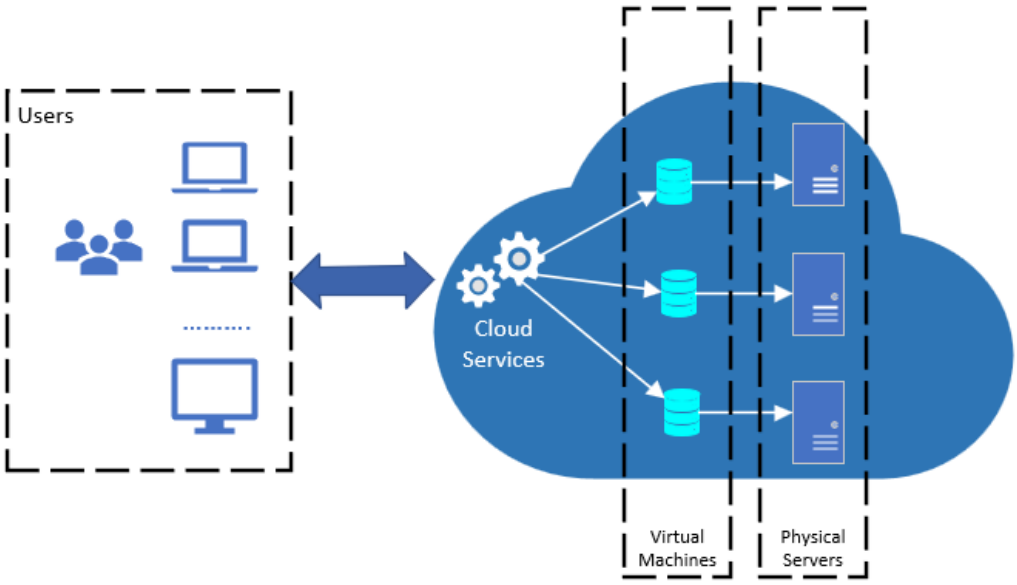

Figure 5.5: Cloud Data Storage Pattern

(Zhang et al., 2020)

This setup in turn means that the security mechanisms used to protect the data are not directly visible to the end user, making it challenging to validate the security of the data storage (Zhang et al., 2020).

The operations performed by the CSP are not directly visible to the users, and can be considered a "black box". This makes it challenging to validate security in Cloud storage, given that Cloud storage will also be subject to the normal internal faults that all compute suffers from - network failures, system malfunctions, software bugs and similar issues (Zhang et al., 2020) (p.5). There is also the challenge associated with commercial incentives: CSP companies are in the Cloud business to make money, and so they have a strong incentive to maximise their profits. This can come at the expense of robust security setups. Cloud service users need ways of validating the confidentiality and reliability of the security mechanisms they have been promised as part of their Cloud subscription. Where the users are in a different legal jurisdiction from the Cloud data centres in which their data is stored, this is even more complex and challenging, both technically and legally. Ascertaining that Cloud data has been secured adequately, and that its confidentiality has been observed,

both require data investigations. Cloud data investigations help validate the trustworthiness of data storage and security mechanisms as applied by a CSP to customer data. These investigations are challenging to carry out reliably when the data centre is in a different jurisdiction - indeed, in some cases it might even be illegal for a customer in a foreign country to be given access to carry out such investigations (Marshall & Rea, 2021).

Disaster Recovery (DR) for Offshored Data is not straightforward. Cloud service subscribers based in small and isolated countries that are reliant on foreign data centres have few options (other than the default subscription models provided by CSPs) when planning Disaster Recovery for their offshored data. Geographical redundancy for such services is also limited to what the CSP can provide. Frequently, this can therefore mean that the subscriber is forced to balance robust DR mechanisms and costs incurred. In the case of New Zealand, this has usually meant choosing between different Cloud Availability Zones based in Australia, which does not provide DR cover in case of Internet link disruptions between New Zealand and Australia (Amazon Web Services, 2024).

The challenges of ensuring adequate Disaster Recovery for offshored data can affect the resilience and availability of systems that depend on it. Isolated countries are dependent on the Submarine Cable Network (SCN) if they are to access foreign-hosted Cloud Services. Besides the challenges posed by natural disasters, this dependence also introduces a further challenge: cable route stress (Payton, 2024). This is an inferred measure of a submarine cable's relative importance. Cable stress tends to be high in regions with limited cable connectivity, such as small and isolated countries, as they rely on a small number of cable routes for their international connectivity.

In the case of New Zealand, for example, cable route stress is quite high due to the country's reliance on a few cable routes to Australia, as shown in the cable maps figure below (Telegeography, 2025b).

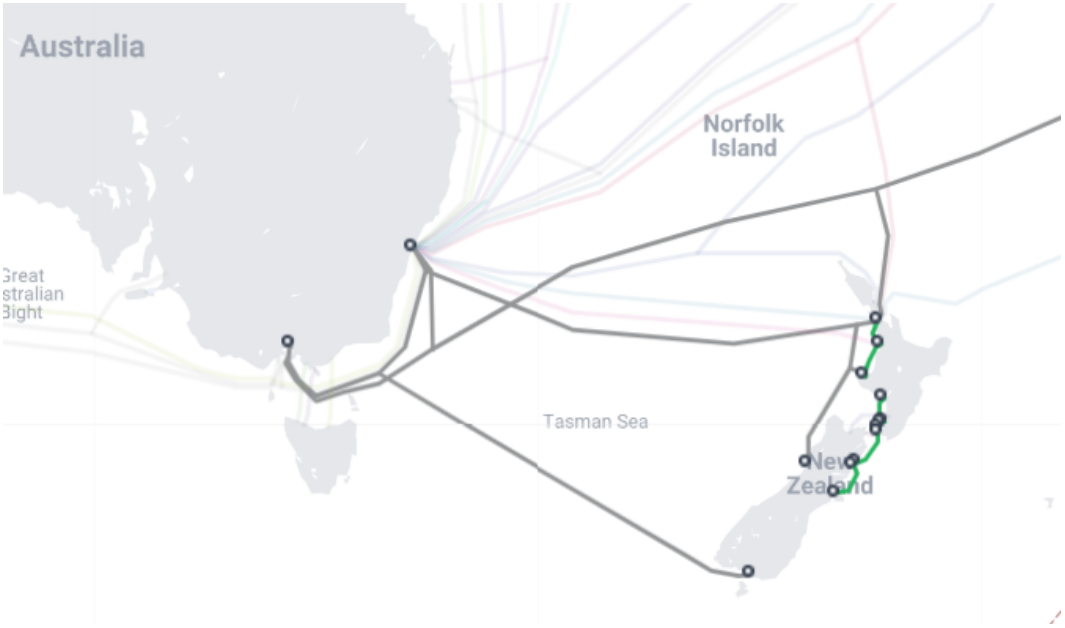

Figure 5.6: New Zealand Undersea Cable Map (Telegeography, 2025b)

This high cable stress in turn imperils the resilience of their Internet connectivity, as any disruption to these routes can lead to prolonged outages and economic losses (Opalinski et al., 2024). For small and isolated countries that lack the resources to invest in redundant cable routes, the risk of prolonged outages is particularly acute and growing.

Geopolitical tensions pose a significant risk for countries that rely on foreign-hosted Cloud Services (Opalinski et al., 2024), and can increase the cable stress already present for small and isolated countries. Undersea cables, which carry the majority of global Internet traffic, are vulnerable to sabotage or accidental damage(Pirenne et al., 2024). Recent incidents of cable cuts in politically volatile regions (Aggarwal, 2025) have highlighted the fragility of international connectivity. Isolated nations dependent on a limited number of cable routes are particularly at risk, as any disruption can lead to prolonged outages and economic losses (Opalinski et al., 2024). The concentration of cloud infrastructure in a few dominant providers further exacerbates this risk, as any disruption to their services can have cascading effects on global connectivity (Moura et al., 2020).

Chapter 6

Recommendations and Conclusion

The rapid adoption of cloud computing has transformed the digital landscape, providing isolated nations with access to scalable and cost-efficient services hosted abroad. However, this reliance on foreign-hosted infrastructure has revealed several challenges that must be addressed to ensure the sustainability and sovereignty of digital services in these regions. The performance issues of latency, jitter, and packet loss, coupled with geopolitical risks and data sovereignty concerns, highlight the need for careful planning and investments. Additionally, such nations face unique barriers due to their geographical remoteness, limited infrastructure, and dependence on a small number of submarine cable routes. To overcome these challenges, it is essential to adopt solutions that reduce reliance on foreign-hosted services, enhance local capabilities, mitigate performance challenges, and build resilient digital ecosystems. The recommendations outlined in this section provide a roadmap for addressing these challenges through targeted technological, infrastructural, and policy interventions.

6.1 Recommendations

1. **Development of Local Data Centres**:

   Isolated nations should prioritise the development of domestic data centres to reduce dependence on foreign-hosted cloud services. As shown in this

work, using local data centres would significantly improve performance by minimise latency, jitter, and packet loss.

From a legal standpoint, using local data centres would enhance digital sovereignty and allow better compliance with local laws (Couture & Toupin, 2019). Investing in local data centres is expensive, but governments can partner with private sector players to attract investments and develop the required infrastructure to support local data centres.

2. **Replication for Disaster Recovery**:

   Disaster Recovery (DR) strategies for users in small and isolated nations are necessarily limited by the connectivity options available in those countries, and the local infrastructure for such a setup. The options all generally involve additional costs, but provide some resilience to disasters that may affect the remote data centre or which may be beyond the control of the user. One of the options available to such users is to replicate the Cloud instance and thus have a measure of DR capability.

3. **Adopting Edge Computing**:

   Leveraging edge computing technology can help bridge the gap between users and centralised cloud services by bringing the processing of data closer to the user (Dang et al., 2021). This approach would reduce latency and improve the performance of time-sensitive applications (Geleji, 2011). This in turn would result in faster response times for applications and faster data processing, both of which are critical for real-time applications such as IoT and telemedicine. Governments should incentivise businesses to adopt and deploy edge computing solutions as part of their digital strategies. Such incentives could include tax breaks and technology training subsidies.

4. **Adoption of Content Delivery Networks (CDNs)**:

   Deploying CDNs can cache data closer to users, improving access speed and reliability, particularly for high-demand applications (Opalinski et

al., 2024). CDNs also enhance the user experience for multimedia content and reduce strain on international bandwidth. Governments can partner with global CDN providers to establish localised nodes that serve their regions. Investing in CDNs is probably beyond the financial means of small countries, but it is possible for regional economic groupings to come together and invest in such facilities for their subregions. As with other investments of this nature, the big Internet companies will need incentives before committing to such significant expenditure, but having a grouping of countries making the case for investment would be better than having each small country trying to make the case on its own.

5. **Investing in Resilient Submarine Cable Infrastructure**:
   Strengthening and diversifying undersea cable connections is critical for improving network reliability (Msongaleli et al., 2015). For small and isolated countries, investing in additional cable routes reduces the risks associated with reliance on a small number of connections (Opalinski et al., 2024). Small countries should also pursue regional collaborations and partnerships so as to share the cost of infrastructure developments. This is particularly attractive for countries in close proximity that share similar digital infrastructure needs. Governments can also explore agreements with global cable providers to ensure the stability of these connections. Where small countries are located in the same wider region (such as the south Pacific, which is dotted with island nations), it makes sense for them to club together in Internet Infrastructure groups and share the financial and logistical burdens of building resilient Submarine Cable Networks. This spreads the cost of such infrastructure and also helps provide geographic redundancy for Internet links for those countries.

6. **Enhancing Legal and Regulatory Frameworks**:
   Governments should establish robust legal frameworks to safeguard data sovereignty (Sharma et al., 2024) and enforce data protection regula-

tions (Digital Government New Zealand, 2024). This includes defining clear rules on cross-border data transfers and ensuring compliance with international privacy standards (Sharma et al., 2024). For small nations without their own Cloud Data Centres, negotiating international agreements to hold foreign cloud providers accountable for data breaches or misuse is also an option (Cochrane, 2021). Small and isolated countries can benefit from international agreements and legislation that defines the minimum standards of legal conformance for big Internet companies. This is outside the realm of pure technology or local solutions, and can possibly be handled at such levels as the United Nations and its regional subgroups. Where such countries lack the legal and technology industry bases needed to take advantage of new technologies, there is a case for some form of aid, similar to economic aid, to support training and investment in Internet infrastructure for those countries.

7. **Public-Private Partnerships**:

   Collaboration between governments and private sectors can accelerate infrastructure development (Mitchell & Samlidis, 2022), as has recently happened with New Zealand and Microsoft (Sorenson, 2024). This includes partnerships for building localised data storage solutions as driven by privacy concerns (Millard, 2015) and establishing high-speed connectivity networks. Normally, robust private sectors can be relied upon to provide the incentives and finances needed for big Internet companies to invest in local data centres. However, the isolation of many small countries and their frequently small economies combine to make this uneconomical for CSPs to invest in such facilities. Public-private partnerships can help overcome these hurdles. For example, a small country could build the physical infrastructure needed for the data centre, and then invite a technology company to set up the servers and networking needed to make it operational.

8. **Incentives for Technology Investments**:

   Policies that incentivise the development of local IT talent, infrastructure, and innovation can help reduce reliance on external providers (Bhatta, 2023). Governments can provide incentives such as tax breaks or grants to attract private sector investments in digital infrastructure. Encouraging universities and technical institutions to collaborate with industry players can also help build a skilled workforce with significant benefits to the country's economy.

9. **Continuous Performance Monitoring**:

   Implementing systems to monitor network performance and data centre access in real-time can help enable the resolution of connectivity disruptions (Palumbo et al., 2021). The use of performance monitoring tools is encouraged, as it can identify bottlenecks and help optimise network traffic (V N Reddy et al., 2022).

6.2 Conclusion

Cloud computing offers significant opportunities for isolated nations to access advanced digital services at reduced costs. However, many of these isolated nations rely on foreign-hosted Cloud services. This introduces challenges such as latency, security vulnerabilities, and legal complexities. This work has demonstrated that these challenges can undermine national digital resilience, economic stability, and sovereignty.

Investing in domestic infrastructure, such as local data centres and resilient submarine cables, can be an important pillar in addressing these challenges. Edge computing and CDNs present additional strategies to improve performance and accessibility for users. By adopting these technologies, isolated nations can reduce their dependency on foreign cloud providers and create a more robust digital ecosystem.

These technologies come at a cost, however, and so collaboration among

governments, the private sector, and international organisations is essential to drive the development of sustainable digital infrastructure. To protect their data, small and isolated nations have to establish legal frameworks that promote digital sovereignty while adhering to global standards. Where they cannot do this independently, it is recommended that they get into partnerships or groupings that can benefit from economies of scale in both investment and regulation. There is also a role to play for the International Community, whose support for small and isolated countries tends to take the form of economic aid and disaster relief (famines, natural disasters, and similar catastrophes). Similar to this, it is clear that the old Digital Divide between wealthy nations and poor ones is once again growing (Cantu-Bazaldua, 2021). With the Internet now being a major contributor to economic development, the aid sent to such countries will need to include technology training and support for infrastructure development. Through careful investments and partnerships, isolated nations can overcome the challenges associated with cloud dependence, and realise the full potential of digital transformation.

Chapter 7

Appendix

Key Technical Terms

The following are key technical terms used in this work:

- **Cloud Services**: Application and infrastructure resources offered as on-demand computing resources such as storage, computing power, applications, and networking over the Internet.
- **Cloud Service Provider (CSP)**: An organisation that offers Cloud Services to subscribers.
- **Content Delivery Network (CDN)**: A system of distributed servers that deliver content to users based on geographic proximity.
- **Edge Computing**: A distributed computing paradigm that brings computation and data storage closer to the location where it is needed.
- **Data Sovereignty**: The concept that data is subject to the laws of the country in which it is located.
- **Data Residency**: The physical location of data.
- **Data Protection**: The process of safeguarding important information from corruption, compromise, or loss.

- **Data Privacy**: The right of an individual to control how their personal information is collected and used.
- **Data Security**: The protection of data from unauthorised access, use, disclosure, disruption, modification, or destruction.
- **Data Breach**: The intentional or unintentional release of secure or private/confidential information to an untrusted environment.
- **Data Loss**: The process of losing information stored on digital media.
- **Data Leak**: The release of secure or private/confidential information to an untrusted environment.
- **Data Encryption**: The process of converting data into a code to prevent unauthorised access.
- **Data Masking**: The process of hiding original data with random characters or data.
- **Disaster Recovery (DR)**: An approach to anticipating and addressing technology-related disasters by preparing for and recovering from adverse events.
- **Isolated Country**: A country that is geographically or geopolitically isolated from the rest of the world.
- **Latency**: Time taken for data to travel from source to destination.
- **Jitter**: Variability in the time it takes for data packets to arrive at their destination.
- **Packet Loss**: Percentage of data packets lost during transmission.
- **Submarine Cable Network (SCN)**: Undersea cables facilitating global Internet connectivity.

References

Aggarwal, M. (2025, January). When american allies' undersea cables are severed, suspicion falls on russia and china [Accessed: 2025-01-21]. https://www.nbcnews.com/news/world/undersea-cables-are-cut-suspicion-falls-russian-chinese-vessels-rcna187105

Amazon Web Services. (2024). Aws global infrastructure map [Accessed: February 17, 2025]. https://aws.amazon.com/about-aws/global-infrastructure/

Astier, H., & Kirby, P. (2024). Germany suspects sabotage behind severed undersea cables [Accessed: 2024-12-17]. https://www.bbc.com/news/articles/c9dl4vxw501o

Australian Competition and Consumer Commission. (2021). News media bargaining code [Accessed: 2024-09-25]. https://www.accc.gov.au/by-industry/digital-platforms-and-services/news-media-bargaining-code/news-media-bargaining-code

Bajpai, V., Eravuchira, S. J., & Schönwälder, J. (2015). Lessons learned from using the ripe atlas platform for measurement research. *SIGCOMM Comput. Commun. Rev.*, *45*(3), 35–42. https://doi.org/10.1145/2805789.2805796

BBC News. (2024). Us-canada border: Tensions rise amid migration surge [Accessed: 2024-09-25]. https://www.bbc.com/news/world-us-canada-67755133

Bhajantri, L. B., & Mujawar, T. (2019). A survey of cloud computing security challenges, issues and their countermeasures. *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*

(I-SMAC), 376–380. https://doi.org/10.1109/I-SMAC47947.2019.9032545

Bhatta, C. (2023). Walking among giants: Foreign policy and development strategies of small and landlocked countries [Accessed: 2024-09-25]. https://www.researchgate.net/profile/Chandra-Bhatta-2/publication/375552352_Walking_among_Giants_Foreign_Policy_and_Development_Strategies_of_Small_and_Landlocked_Countries/links/654e65f5b86a1d521bcc2ad3/Walking-among-Giants-Foreign-Policy-and-Development-Strategies-of-Small-and-Landlocked-Countries.pdf

BITAG. (2022). Latency explained - broadband internet technical advisory group [Accessed: March 06, 2025.]. https://www.bitag.org/documents/BITAG_latency_explained.pdf

Bowen, J., & Hinze, A. (2022). Participatory data design: Managing data sovereignty in iot solutions. *Interacting with Computers*, *34*(2), 60–71. https://doi.org/10.1093/iwc/iwac031

Cantu-Bazaldua, F. (2021). Remote but well connected? neighboring but isolated? measuring remoteness in the context of small island developing states. *UNCTAD Research Paper No. 67*.

Carter, L., Burnett, D., Drew, S., Marle, G., Hagadorn, L., Bartlett-McNeil, D., & Irvine, N. (2009). *Submarine cables and the oceans – connecting the world*. ICPC/UNEP/UNEP-WCMC. http://www.iscpc.org/publications/icpc-unep_report.pdf

Charyyev, B., Arslan, E., & Gunes, M. H. (2020). Latency comparison of cloud datacenters and edge servers. *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 1–6. https://doi.org/10.1109/GLOBECOM42002.2020.9322406

Chen, K.-T., Huang, P., & Lei, C.-L. (2009). Effect of network quality on player departure behavior in online games. *IEEE Transactions on Parallel and Distributed Systems*, *20*(5), 593–606. https://doi.org/10.1109/TPDS.2008.148

Cherrington, M., Airehrour, D., Lu, J., Xu, Q., Wade, S., & Dunn, I. (2020). Indigenous big data implications in new zealand. *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, 1–6. https://doi.org/10.1109/ITNAC50341.2020.9315078

Cochrane, T. (2021). Law enforcement cross-border data sharing: A cloud act agreement for new zealand? *New Zealand Law Review*, *2021*(3), 401–434. https://www.ingentaconnect.com/contentone/lrf/nzlr/2021/00002021/00000003/art00002?crawler=true&mimetype=application/pdf

Cory, N. (2017, May). Cross-border data flows: Where are the barriers, and what do they cost? https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/

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

Dang, T. K., Mohan, N., Corneo, L., Zavodovski, A., Ott, J., & Kangasharju, J. (2021). Cloudy with a chance of short rtts: Analyzing cloud connectivity in the internet. *Proceedings of the 21st ACM Internet Measurement Conference*, 62–79. https://doi.org/10.1145/3487552.3487854

Digital Government New Zealand. (2024, December). Cloud jurisdictional risk guidance [Accessed: 2024-12-17].

Dillon, S., & Vossen, G. (2015). Saas cloud computing in small and medium enterprises: A comparison between germany and new zealand. *International Journal of Information Technology, Communications and Convergence*, *3*(2), 87–104. https://doi.org/10.1504/IJITCC.2015.070998

El Makkaoui, K., Ezzati, A., & Hssane, A. B. (2015). Challenges of using homomorphic encryption to secure cloud computing. *2015 International Conference on Cloud Technologies and Applications (CloudTech)*, 1–7. https://doi.org/10.1109/CloudTech.2015.7337011

European Telecommunications Standards Institute (ETSI). (2008, August). *Speech Processing, Transmission and Quality aspects (STQ); User related QoS parameter definitions and measurements; Part 4 - Internet Access* (ETSI Guide (EG) No. EG 202 057-4 V1.2.1). ETSI. https://www.etsi.org/deliver/etsi_eg/202000_202099/20205704/01.02.01_60/eg_20205704v010201p.pdf

Galij, S., et al. (2024). Modeling data sovereignty in public cloud—a comparison of existing solutions [Accessed 2025-02-06]. *Applied Sciences*, *14*(23). https://doi.org/10.3390/app142310803

Gamero-Garrido, A., Carisimo, E., Hao, S., Huffaker, B., Snoeren, A. C., & Dainotti, A. (2021). Quantifying nations exposure to traffic observation and selective tampering. *CoRR*, *abs/2110.05772*. https://arxiv.org/abs/2110.05772

GeeksforGeeks. (2024). Difference between ping and traceroute [Accessed: March 03, 2025.]. https://www.geeksforgeeks.org/difference-between-ping-and-traceroute/

Geleji, G. (2011). *On multi-domain qos routing and rate jitter analysis* [Doctoral dissertation] [AAI3497245]. North Carolina State University.

Hu, F., Liu, Q., Wu, J., & Yao, J. (2019). Minimizing geo-distributed interactive service cost with multiple cloud service providers. *IEEE Access*, *7*, 3320–3335. https://doi.org/10.1109/ACCESS.2018.2883964

Hudson, H. E. (2011). Reaching the cloud: Broadband strategies for small states and developing regions. *2011 Technical Symposium at ITU Telecom World (ITU WT)*, 211–216.

Ibm adds watsonx service to ibm cloud in australia and new zealand. (2024). *ICT Monitor Worldwide*. https://ezproxy.waikato.ac.nz/login?url=https://www.proquest.com/wire-feeds/ibm-adds-watsonx-service-cloud-australia-new/docview/3133830251/se-2

Inc, E. (2024). Data location considerations. https://pro.arcgis.com/en/pro-app/latest/get-started/data-locations.htm

Jansen, B., Kadenko, N., Broeders, D., van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, *40*(4), 101862. https://doi.org/https://doi.org/10.1016/j.giq.2023.101862

Jia, J., & Wang, P. (2022). Low latency deployment of service-based data-intensive applications in cloud-edge environment, 57–66. https://doi.org/10.1109/ICWS55610.2022.00023

Kirschenbaum, A. (2018). Beyond microsoft: A legislative solution to the sca's extraterritoriality problem. *Fordham Law Review*, *86*(4), 1923–1962. https://heinonline.org/HOL/Page?handle=hein.journals/flr86&collection=journals&id=1960&startid=1960&endid=1999

Kobayashi, M. (2014). Experience of infrastructure damage caused by the great east japan earthquake and countermeasures against future disasters. *IEEE Communications Magazine*, *52*(3), 23–29. https://doi.org/10.1109/MCOM.2014.6766080

Kodali, S. S. P., Podili, P., & Kataoka, K. (2019). Tagging based packet loss detection and recovery of ip multicast in sdn. *Proceedings of the 15th Asian Internet Engineering Conference*, 17–24. https://doi.org/10.1145/3340422.3343637

Koske, I., Bitetti, R., Wanner, I., & Sutherland, E. (2014). The internet economy - regulatory challenges and practices. (1171). https://doi.org/https://doi.org/https://doi.org/10.1787/5jxszm7x2qmr-en

Kshetri, N. (2010). Cloud computing in developing economies. *Computer*, *43*(10), 47–55. https://doi.org/10.1109/MC.2010.212

Kumar, R., Carisimo, E., Riva, L. D. A., Buzzone, M., Bustamante, F. E., Qazi, I. A., & Beiró, M. G. (2024). Of choices and control - a comparative analysis of government hosting. *Proceedings of the 2024 ACM on Internet Measurement Conference*, 462–479. https://doi.org/10.1145/3646547.3688447

Kushwaha, N., Roguski, P., & Watson, B. W. (2020). Up in the air: Ensuring government data sovereignty in the cloud. *2020 12th International Conference on Cyber Conflict (CyCon)*, *1300*, 43–61. https://doi.org/10.23919/CyCon49761.2020.9131718

Lai, Y.-C., Kao, C.-C., Jhan, J.-D., Kuo, F.-H., Chang, C.-W., & Shih, T.-C. (2020). Quality of service measurement and prediction through ai technology. *2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)*, 254–257. https://doi.org/10.1109/ECICE50847.2020.9302008

Maheshwari, S., Raychaudhuri, D., Seskar, I., & Bronzino, F. (2018). Scalability and performance evaluation of edge cloud systems for latency constrained applications. *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, 286–299. https://doi.org/10.1109/SEC.2018.00028

Marshall, K., & Rea, A. (2021, August). *Legal challenges in cloud forensics*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1341&context=amcis2021

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: An enterprise perspective on risks and compliance*. OReilly Media, Inc.

Microsoft. (2025a, January). Australia east azure cloud zone [Accessed: 2025-01-15]. https://datacenters.microsoft.com/globe/explore?info=region_australiaeast

Microsoft. (2025b, January). West us azure cloud zone [Accessed: 2025-01-15]. https://datacenters.microsoft.com/globe/explore?info=region_westus

Millard, C. (2015). Forced localization of cloud services: Is privacy the real driver? *IEEE Cloud Computing*, *2*(2), 10–14. https://doi.org/10.1109/MCC.2015.37

Mitchell, A. D., & Samlidis, T. (2022). Cloud services and government digital sovereignty in australia and beyond. *International Journal of Law and Information Technology*, *29*(4), 364–394. https://doi.org/10.1093/ijlit/eaac003

Moura, G. C. M., Castro, S., Hardaker, W., Wullink, M., & Hesselman, C. (2020). Clouding up the internet: How centralized is dns traffic becoming? *Proceedings of the ACM Internet Measurement Conference*, 42–49. https://doi.org/10.1145/3419394.3423625

Msongaleli, D. L., Dikbiyik, F., Zukerman, M., & Mukherjee, B. (2015). Disaster-aware submarine fiber-optic cable deployment. *2015 International Conference on Optical Network Design and Modeling (ONDM)*, 245–250. https://doi.org/10.1109/ONDM.2015.7127306

Murphy, J. (2011). Performance engineering for cloud computing. In N. Thomas (Ed.). Springer Berlin Heidelberg.

Mutkoski, S. (2015). National cloud computing principles: Guidance for public sector authorities moving to the cloud. *2015 IEEE International Conference on Cloud Engineering*, 404–409. https://doi.org/10.1109/IC2E.2015.104

Obren, M., & Howell, B. (2014). The tyranny of distance prevails: Http protocol latency and returns to fast fibre internet access network deployment in remote economies. *The Annals of Regional Science*, *52*(1), 65–85. https://doi.org/10.1007/s00168-013-0574-0

Opalinski, N., Uzmi, Z., & Douzet, F. (2024). The quest for a resilient internet access in a constrained geopolitical environment. *Proceedings of the Asian Internet Engineering Conference 2024*, 55–66. https://doi.org/10.1145/3674213.3674220

Palumbo, F., Aceto, G., Botta, A., Ciuonzo, D., Persico, V., & Pescapé, A. (2021). Characterization and analysis of cloud-to-user latency: The case of azure and aws. *Computer Networks*, *184*, 107693. https://doi.org/https://doi.org/10.1016/j.comnet.2020.107693

Payton, B. (2024). Severed internet cables highlight africa's vulnerability: Many african countries are particularly vulnerable to damage to the cables that carry most internet traffic, as ben payton says in this guest column. *African Business*, (512), 82. https://link-gale-com.ezproxy.

waikato . ac . nz / apps / doc / A791604963 / AONE ? u = waikato & sid = googleScholar&xid=86d2b478

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems and Software*, *103*, 167–181. https://doi.org/https://doi.org/10.1016/j.jss.2015.02.002

Pirenne, B., Moran, K., & Howe, B. (2024). Real-time, year-round, cross-arctic observations integrating three complementary technologies into submarine telecommunication cables. *OCEANS 2024 - Halifax*, 1–4. https://doi.org/10.1109/OCEANS55160.2024.10753815

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Ray, D., Bobadilla Riquelme, V., & Seshan, S. (2022). Prism: Handling packet loss for ultra-low latency video. *Proceedings of the 30th ACM International Conference on Multimedia*, 3104–3114. https://doi.org/10.1145/3503161.3547856

Schlinker, B., Cunha, I., Chiu, Y.-C., Sundaresan, S., & Katz-Bassett, E. (2019). Internet performance from facebook's edge. *Proceedings of the Internet Measurement Conference*, 179–194. https://doi.org/10.1145/3355369.3355567

Schwartz, P. M. (2018). Legal access to the global cloud. *Columbia Law Review*, *118*(6), 1681–1762. Retrieved December 19, 2024, from https://www.jstor.org/stable/26511248

Sermpezis, P., Prehn, L., Kostoglou, S., Flores, M., Vakali, A., & Aben, E. (2023). Bias in internet measurement platforms. *2023 7th Network Traffic Measurement and Analysis Conference (TMA)*, 1–10. https://doi.org/10.23919/TMA58422.2023.10198985

Sharma, P., Martin, M., Swanlund, D., Latham, C., Anderson, D., & Wood, W. (2024). A cloud-based solution for trustless indigenous data sovereignty: Protecting māori biodiversity management data in aotearoa new

zealand. *Transactions in GIS*, *28*(4), 836–857. https://doi.org/https://doi.org/10.1111/tgis.13153

Shreya, J. L., & Saini, A. (2023). Delay analysis in programmable data plane using jitter calculations. *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing*, 683–691. https://doi.org/10.1145/3607947.3608083

Smith, S. C., Hammell, R. J., & Wong, K. W. (2016). An experimental exploration of the impact of host-level packet loss on network intrusion detection, 13–19. https://doi.org/10.1109/CYBERSEC.2016.010

Sorenson, V. (2024, December). New zealand's first hyperscale cloud is open for business [Accessed: 2024-12-17]. https://news.microsoft.com/en-nz/2024/12/12/new-zealands-first-hyperscale-cloud-is-open-for-business/

Speedtest by Ookla. (2025, February). Speedtest result id 17396540350 [Accessed: 19-Feb-2025]. https://www.speedtest.net/result/17396540350

Submarine Networks Company Ltd. (2025, January). New zealand undersea cables [Accessed: 2025-01-16]. https://www.submarinenetworks.com/en/stations/oceania/new-zealand

Susantha, K., Lu, D., & Wang, X. (2023). Lessons learned from previous cyber-attacks on energy systems – global and australian context. *2023 IEEE International Future Energy Electronics Conference (IFEEC)*, 550–554. https://doi.org/10.1109/IFEEC58486.2023.10458537

Swinhoe, D. (2024, April). The houthis and the red sea: A new risk to subsea cables. https://www.datacenterdynamics.com/en/analysis/the-houthis-and-the-red-sea-a-new-risk-to-subsea-cables/

Te Mana Raraunga. (2025). Our māori data sovereignty principles [Accessed: 2025-07-14]. https://www.temanararaunga.maori.nz/nga-rauemi

Telegeography. (2025a, January). Kenya submarine cable map [Accessed: 2025-01-22]. https://www.submarinecablemap.com/landing-point/auckland-new-zealand

Telegeography. (2025b, January). New zealand submarine cable map [Accessed: 2025-01-22]. https://www.submarinecablemap.com/landing-point/auckland-new-zealand

The Guardian. (2024). Elon musk's x faces calls for brazil block after disinformation warnings [Accessed: 2024-09-25]. https://www.theguardian.com/technology/2024/sep/18/elon-musks-x-brazil-block

Times, T. N. Y. (2022). How russia took over ukraine's internet in occupied territories. *The New York Times*. https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html

Tod, C. (2022). New zealand internet connectivity to aws [Accessed 14-08-2024]. https://aws.amazon.com/blogs/architecture/new-zealand-internet-connectivity-to-aws/

Tongsuksai, S., Mathrani, S., & Weerasinghe, K. (2023). Influential characteristics and benefits of cloud erp adoption in new zealand smes: A vendors' perspective. *IEEE Access*, *11*, 23956–23979. https://doi.org/10.1109/ACCESS.2023.3254500

V N Reddy, A., Kumar, A. A., Venu, N., & Vijaya Kumar Reddy, R. (2022). On optimization efficiency of scalability and availability of cloud-based software services using scale rate limiting algorithm. *Measurement: Sensors*, *24*, 100468. https://doi.org/https://doi.org/10.1016/j.measen.2022.100468

Wang, X., Wang, Z., Wang, T., & Zukerman, M. (2023). Designing cost-effective and reliable submarine communications cable path: Lessons from the tonga volcano disaster. *IEEE Communications Magazine*, *61*(7), 179–185. https://doi.org/10.1109/MCOM.008.2200512

Wu, W., Bischof, Z. S., Testart, C., & Dainotti, A. (2024). Poster: Enhancing internet disruption investigation via path monitoring. *Proceedings of the 2024 ACM on Internet Measurement Conference*, 777–778. https://doi.org/10.1145/3646547.3689675

Yang, H., Pan, H., & Ma, L. (2023). A review on software defined content delivery network: A novel combination of cdn and sdn. *IEEE Access*, *11*, 43822–43843. https://doi.org/10.1109/ACCESS.2023.3267737

Zaki, Y., Chen, J., Pötsch, T., Ahmad, T., & Subramanian, L. (2014). Dissecting web latency in ghana. *Proceedings of the 2014 Conference on Internet Measurement Conference*, 241–248. https://doi.org/10.1145/2663716.2663748

Zhang, Y., Xu, C., & Shen, X. ((2020). *Data security in cloud storage* (1st ed. 2020.). Springer Singapore.

Zhao, Y., Wu, Q., Lv, G., Yang, F., Zhang, J., Peng, F., Liu, Y., Li, Z., Chen, Y., Guo, H., & Xie, G. (2024). Jitbright: Towards low-latency mobile cloud rendering through jitter buffer optimization. *Proceedings of the 34th Edition of the Workshop on Network and Operating System Support for Digital Audio and Video*, 36–42. https://doi.org/10.1145/3651863.3651881

Zheng, Y., & Gong, B. (2024). Nexus between natural resources and digital economy: The role of geopolitical risk. *Resources Policy*, *89*, 104600. https://doi.org/https://doi.org/10.1016/j.resourpol.2023.104600