DNS Dependencies as an Expression of the Digital Divide: the Example of Australia

Niousha Nazemi
Omid Tavallaie
Albert Y. Zomaya
Ralph Holz

Summary

This study investigates the relationship between DNS dependencies and the digital divide in Australia by analyzing Australian government websites providing services to the general population and indigenous populations.

Introduction

The **digital divide** refers to a gap between groups

Some groups have access to, and can use, digital technologies effectively - while others cannot.

This includes **access** to the internet

Having access to the internet provides opportunities that those without access do not have.

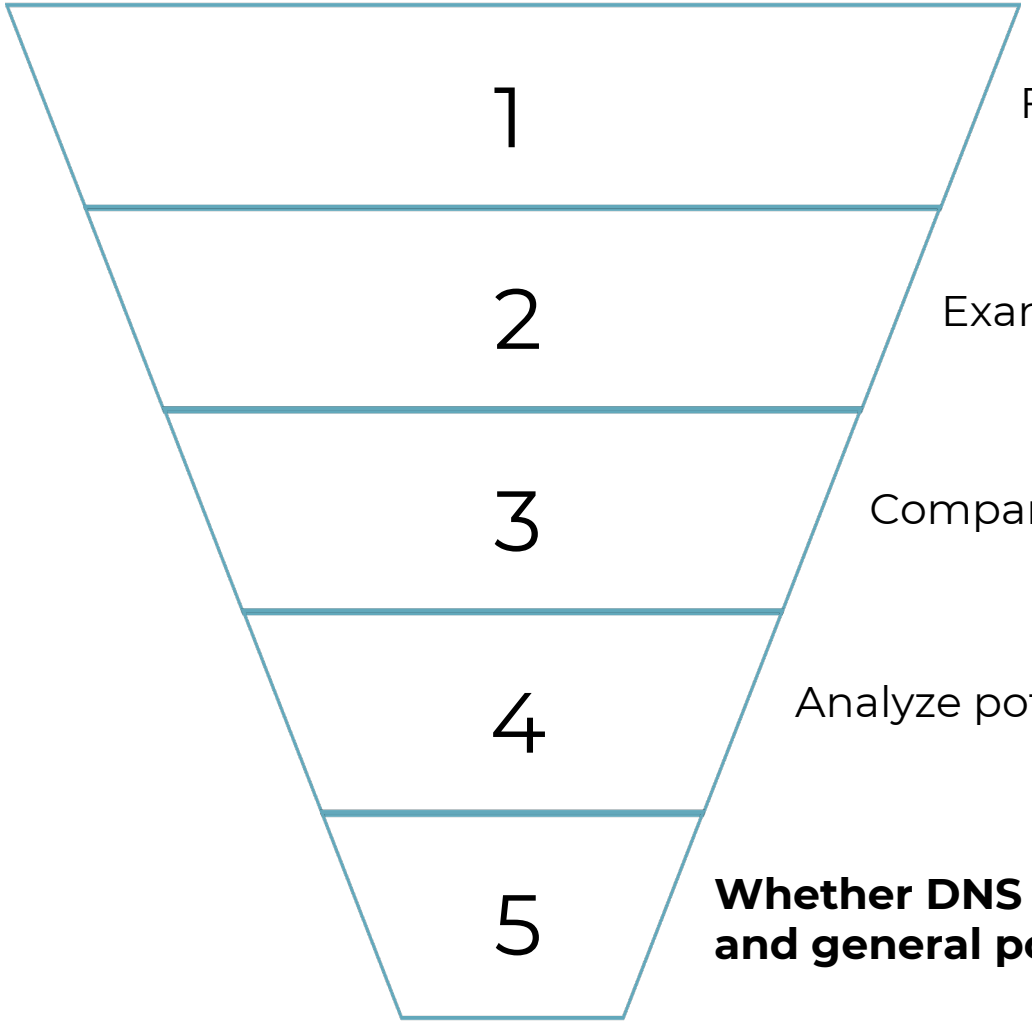
Every service has **DNS dependencies**

Resilience on services depends on third-party providers.

Internet transparency refers to understanding

How the Internet works
E.g., revealing critical Internet dependencies.

Research Question



Focus on indigenous communities in Australia

Examine DNS dependencies for government websites

Compare DNS dependencies for domains of indigenous vs general group

Analyze potential impacts on access and resilience

Whether DNS dependencies reflect a digital divide between indigenous and general populations in Australia.

Methodology

The methodology involves:

- Creating lists of domain names of Australian government websites that provide services for the indigenous population and the general population.
- Retrieving authoritative nameservers of the domains to identify delegation
- Exposing DNS dependencies
- Categorizing domains based on their DNS provider dependencies.

Differences in DNS Setups

USE OF HYPER-SCALERS

USE OF DOMESTIC PROVIDERS

USE OF GOVERNMENT-OWNED PROVIDERS

MULTI-DNS PROVIDER SETUP

Digital Divide and DNS dependencies

More non-leading providers for indigenous domains

46.3% of indigenous domains use smaller, often domestic Australian DNS providers compared to general population

Few domains use multi-provider strategy

Only 8% of general domains and none of the indigenous domains use redundancy through multi-provider DNS

No indigenous domains used intra-gov DNS providers, unlike over 25% of general population domains

While over 100 general population domains leveraged DNS provided by government sector, none of the indigenous domains did.

Around half of the domains for both populations used leading DNS providers

Leading DNS providers like Amazon, Microsoft and Cloudflare were used by about 50% of domains for both general and indigenous populations.

Preference of domestic providers for Indigenous sites

Use more domestic and smaller providers

Fewer leading DNS providers and less diversity for indigenous domains

Indigenous domains utilized fewer leading DNS providers overall, with heavier reliance on Microsoft, and more use of smaller Australian providers.

Implications

Less redundancy

Indigenous domains have no multi-provider setups, indicating less redundancy. That may indicate desire for better DNS but inability to use cloud.

Single point of failure

With only single providers, indigenous domains have a single point of failure.

Lack of government support

No indigenous domains use government DNS providers, suggesting less support.

Fewer resources

Less use of leading providers indicates fewer resources.

More reliance on domestic providers

Indigenous domains use more domestic providers, implying less access to global services.

Early work! Limitations!

Indirect Dependencies

Higher level DNS delegations impact availability and security. Analysis of indirect dependencies is preliminary.

Longitudinal Study Needed

A snapshot study has limitations. Longitudinal observations over time would reveal dynamics of DNS provisioning.

Small Indigenous Sample Size

The indigenous sample is much smaller than the general population sample. Small samples require caution in comparison.

Specific Australian Focus

The study focuses specifically on Australian indigenous governmental domains. The methodology could be adapted more broadly.

Other Forms of Outsourcing

The study currently examines DNS names and WHOIS data. Further work should investigate IP address ownership.

Conclusion

- Some evidence for digital divide
- There are clear differences in DNS dependencies between general and indigenous domains in Australia, signaling a digital divide.

- Centralization increases vulnerability
  Consolidation of DNS providers makes systems prone to single point of failure

- Differing DNS setups matter
  DNS dependencies and configurations impact service availability across groups.

Future Research

- Analyze services supported by government DNS
  Identify the types of websites and services hosted on government-run DNS infrastructure.

- Government systems
  Investigate why government-hosted providers are used for some groups but not indigenous groups

- Local providers
  Study how availability and control differ between local Australian providers versus international hyper-scalers

- Resilience
  Assess how indigenous groups can gain more resilient and redundant DNS infrastructure through multiple providers

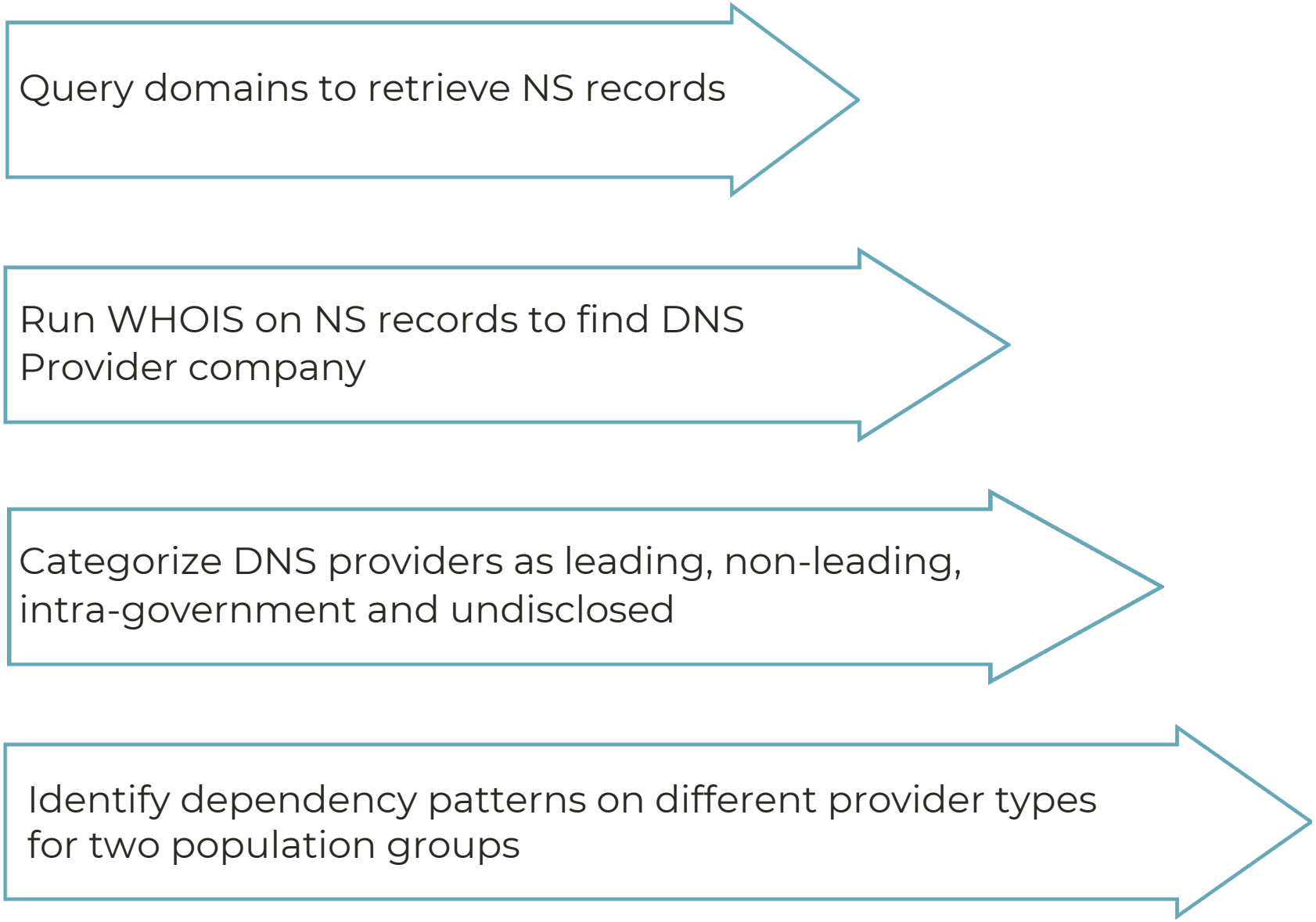
- Monitor long-time availability and provider changes
  Track website uptime and DNS provider transitions over an extended period.

- Investigate other forms of dependencies
  Examine how websites depend on other services like content delivery networks and web hosting providers

Thank You

Q & A

DNS Dependencies

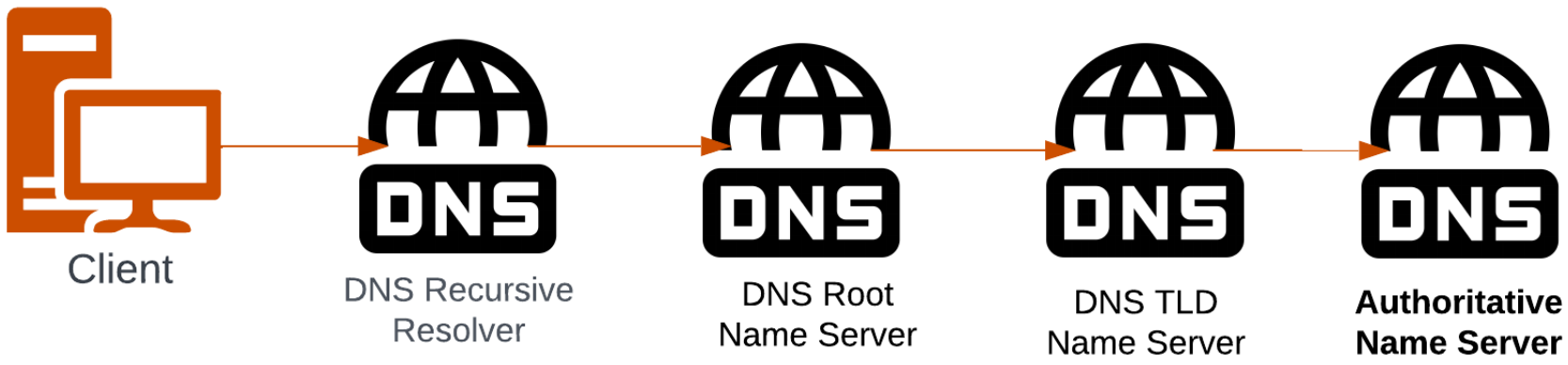


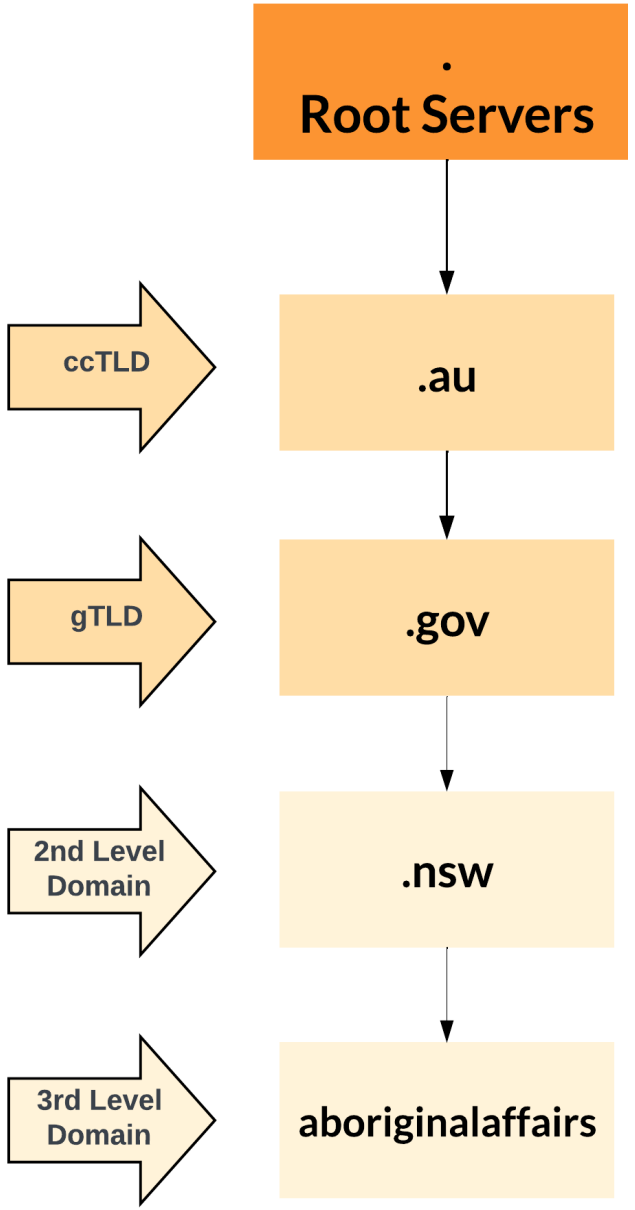
Results - Dependency on third-party DNS providers

Population group	General		Indigenous	
	Absolute	Relative	Absolute	Relative
Number of domains	448	100%	54	100%
Depends on...				
...leading providers	219	48.9%	29	53.7%
...non-leading providers	140	31.3%	25	46.3%
...intra-government providers	113	25.2%	0	
...single provider	412	92%	54	100%
...multiple providers	36	8%	0	0
...intra-government + 3rd party providers	19	4.2%	0	0
Undisclosed	8	1.8%	0	0

DNS (Domain Name System)

DNS is a hierarchical system that translates human-readable domain names into IP addresses.





Related Work

Industry consolidation

The DNS industry is undergoing consolidation, reducing diversity of providers.

Infrastructure concentration

Internet infrastructure is becoming increasingly concentrated among a few organizations.

Key DNS providers

Studies reveal the dominance of a few key DNS providers due to centralization and consolidation.

DNS traffic impact

Centralization impacts DNS traffic, leading to vulnerabilities like TsuNAME that cause traffic escalation.

Service disruption

Centralization introduces vulnerabilities that can lead to DNS service disruptions.

DNS Misconfigurations

Research has found government domains vulnerable to DNS misconfigurations, which can lead to service degradation or interruption.

Defective Delegations

Government domains can be vulnerable to hijacking due to defective delegations and over reliance on a single third-party DNS service provider.

Indigenous Communities in Australia

Two Main Groups

- Aboriginal Australians
- Torres Strait Islanders

Digital Divide

Indigenous communities in Australia face challenges accessing digital information and acquiring skills for effective technology utilization.

Economic Disadvantage

A digital divide often affects already economically disadvantaged groups, including indigenous communities in Australia.

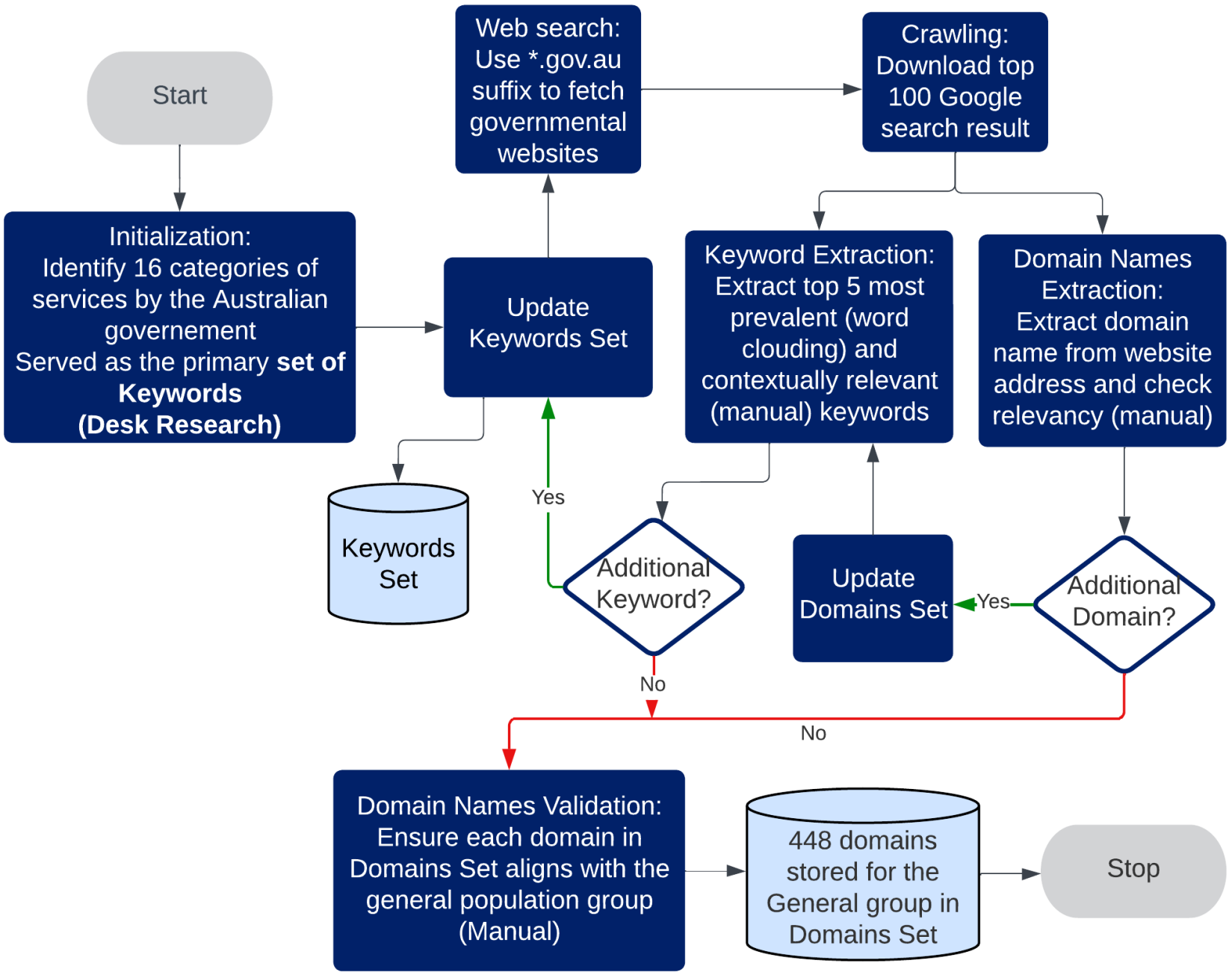
Geographic Dispersion

Indigenous communities are often geographically dispersed, so digital divides can significantly impact access to services.

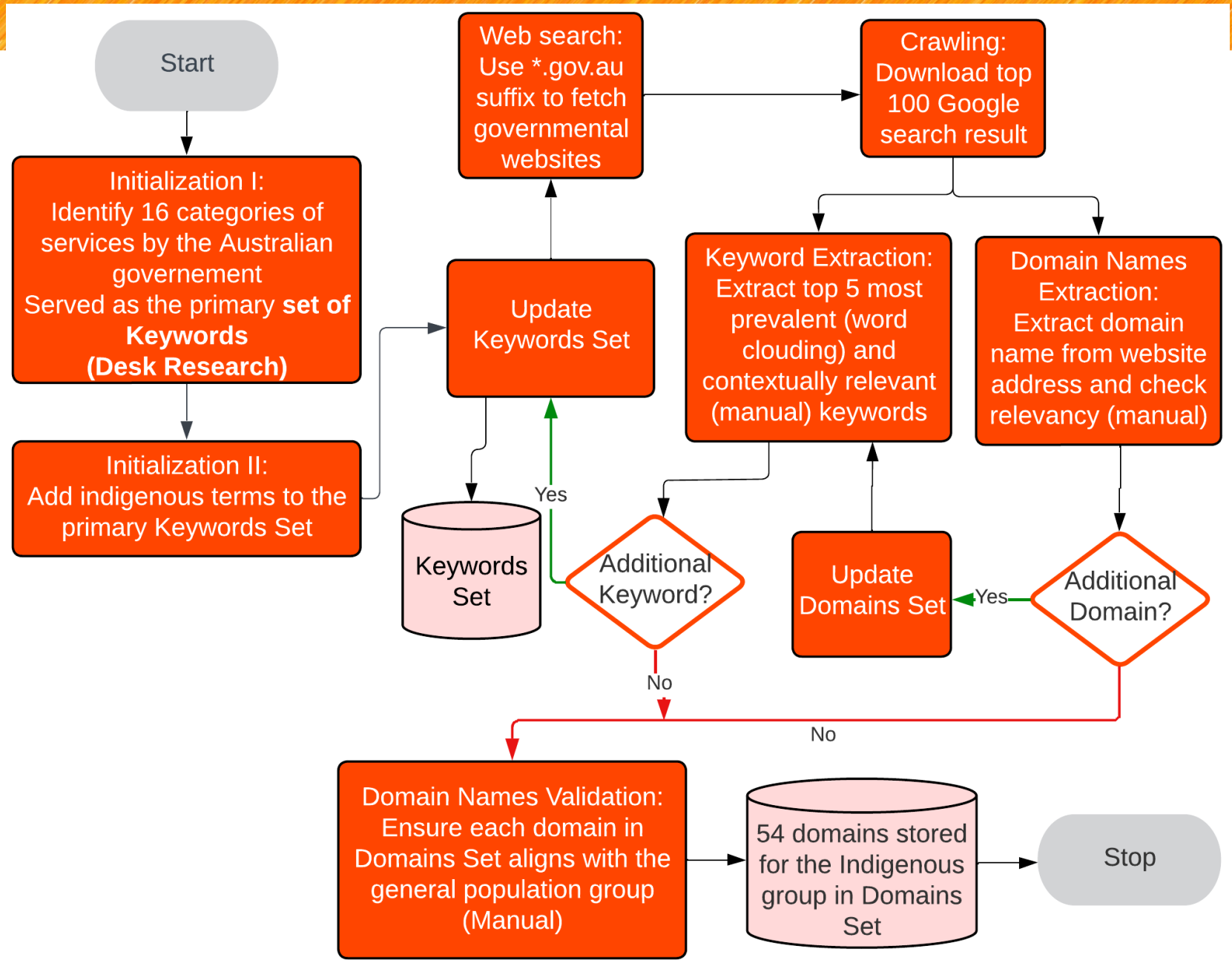
Dependency on Few Providers

Centralization of core infrastructure like DNS increases reliance on few providers, affecting access for disadvantaged groups.

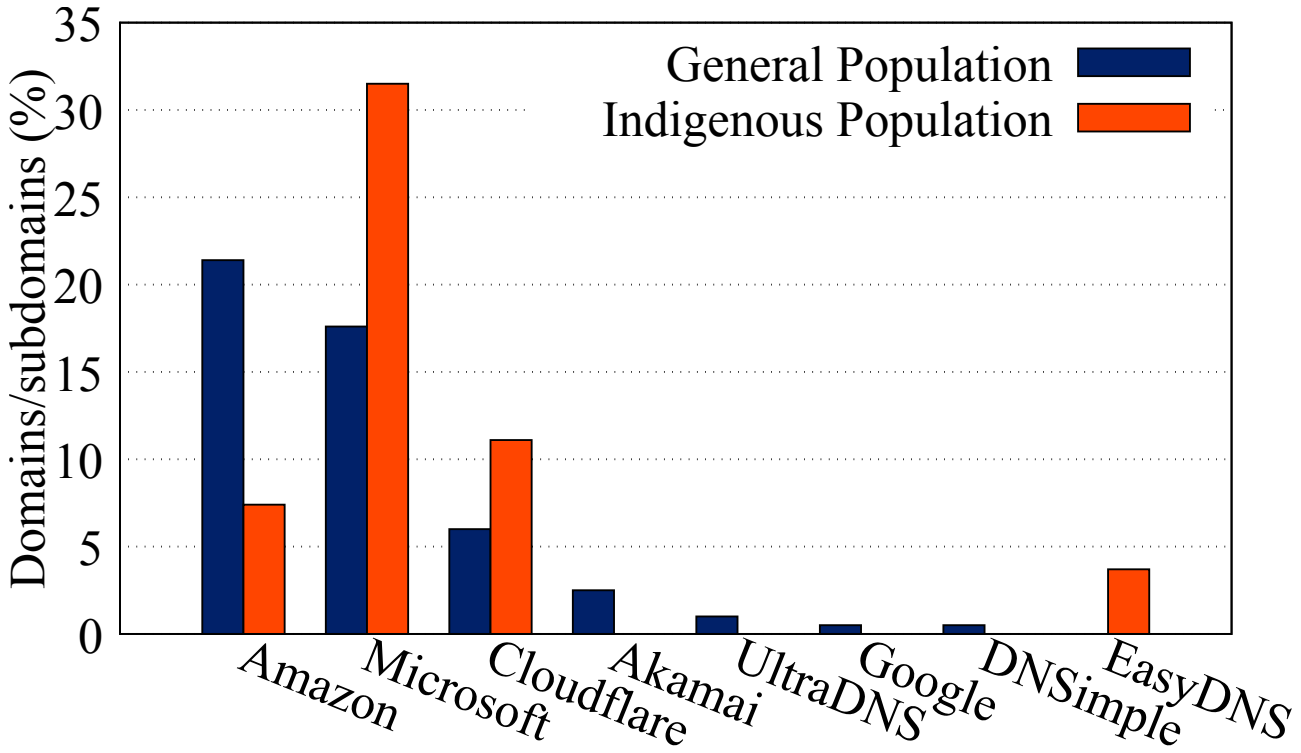
Data Collection – Domains for General People



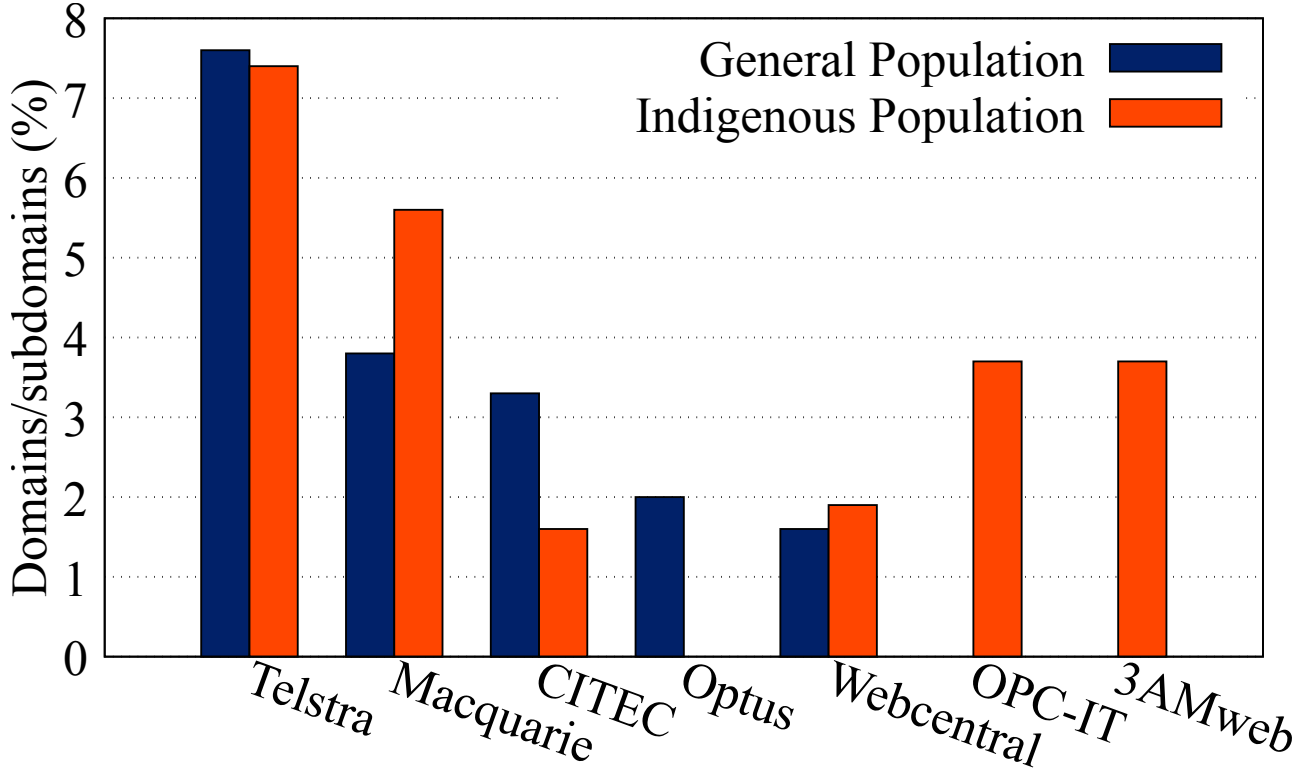
Data Collection – Domains for Indigenous People

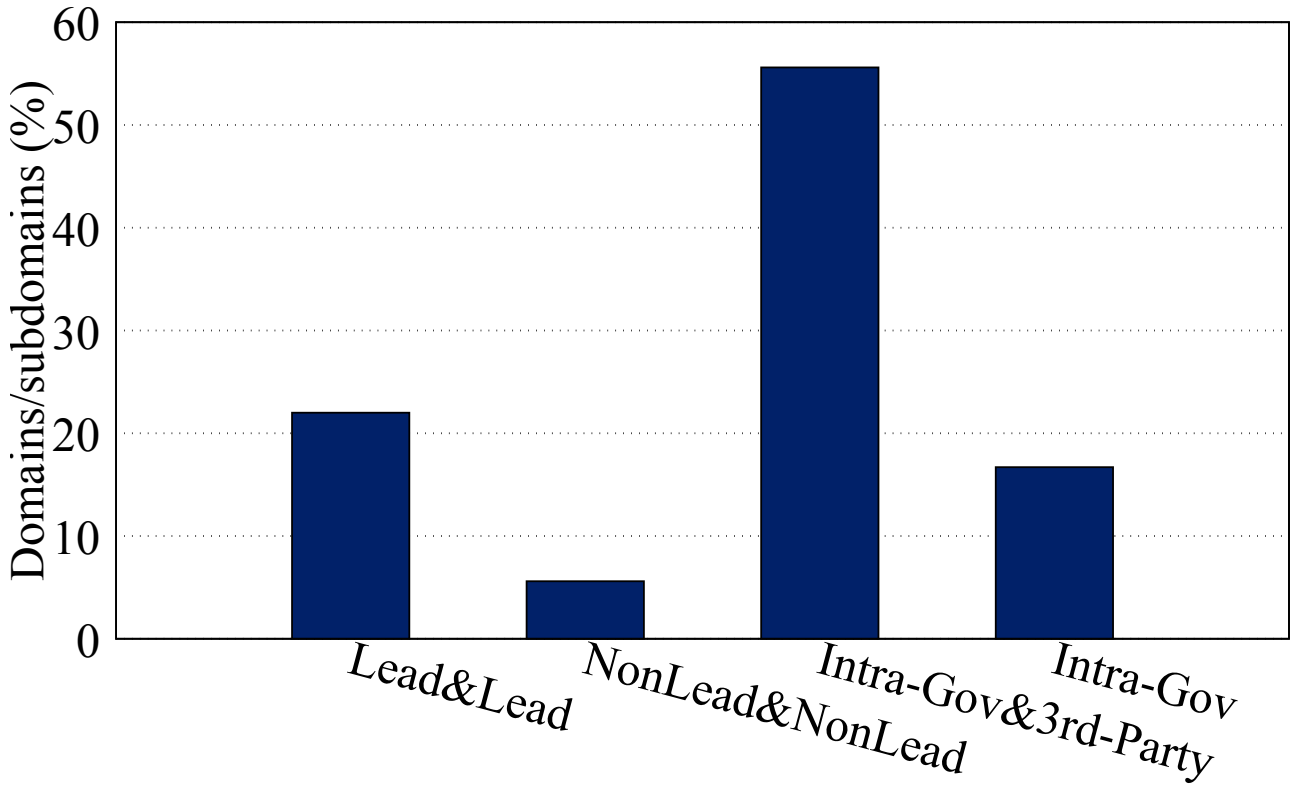


Use of leading DNS providers



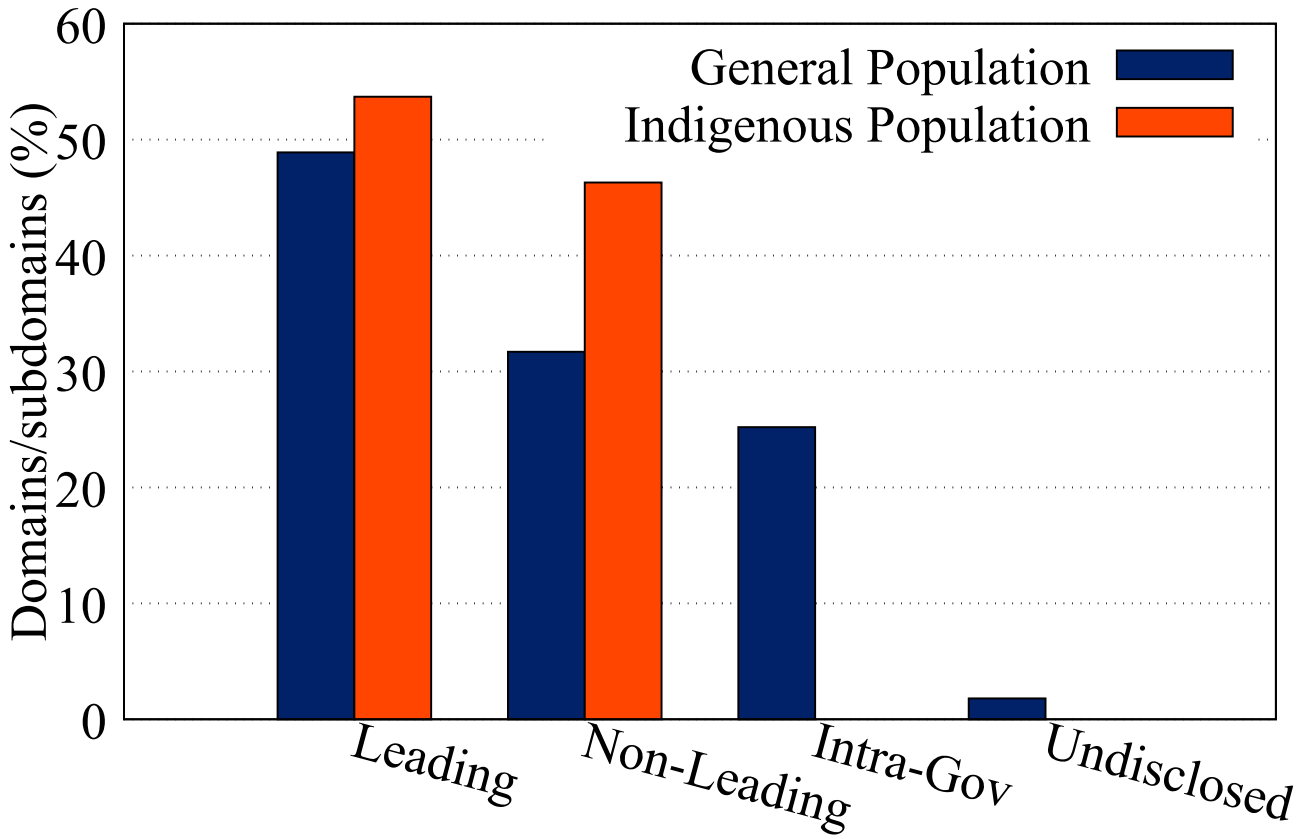
Use of domestic DNS providers





Multi-DNS setups (only general population)

DNS providers by category



Use of non-leading DNS providers