Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services

Agung Septiadi
University of New South Wales
Sydney, NSW, Australia

Minzhao Lyu
University of New South Wales
Sydney, NSW, Australia

Hassan Habibi Gharakheili
University of New South Wales
Sydney, NSW, Australia

Vijay Sivaraman
University of New South Wales
Sydney, NSW, Australia

Abstract

Online government services are increasingly regarded as critical national functions, yet their supporting infrastructures remain vulnerable to outages caused by natural disasters, geopolitical tensions, and targeted attacks. Central to their operation is the authoritative Domain Name System (DNS) infrastructure, the single source of truth that maps government domain names to service endpoints. In this paper, we introduce a comprehensive assessment framework to systematically evaluate the operational resilience of authoritative DNS infrastructure per government service. Our first contribution develops a data schema that characterizes a domain's authoritative DNS infrastructure across four hierarchical levels: entire hosting infrastructure, server functionality, name servers, and hosting instances. Our second contribution identifies resilience attributes at their finest hierarchy across three operational phases, namely infrastructure placement, service configuration, and DNS record dispatch. Numerical scores are assigned and aggregated algorithmically to enable consistent and cross-domain comparisons. Lastly, we apply our method to government domains in six representative countries.

CCS Concepts

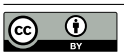
• **Networks** → **Network measurement**; • **Security and privacy** → **Network security**; • **Computing methodologies** → *Modeling and simulation.*

Keywords

Domain name system; authoritative DNS; network resilience

ACM Reference Format:
Agung Septiadi, Minzhao Lyu, Hassan Habibi Gharakheili, and Vijay Sivaraman. 2026. Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services. In *Abstracts of the 2026 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS Abstracts '26), June 08–12, 2026, Ann Arbor, MI, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3801489.3806862

Corresponding author: Minzhao Lyu (minzhao.lyu@unsw.edu.au).
The full version of this SIGMETRICS paper is available at [4].



SIGMETRICS Abstracts '26, Ann Arbor, MI, USA

ACM ISBN 979-8-4007-2570-8/2026/06
https://doi.org/10.1145/3801489.3806862

1 Overview

Disruptions to government digital infrastructure that arise from various causes, ranging from natural disasters to cyberattacks, constitute high-priority incidents for national and local authorities. Unfortunately, such disruptions are not uncommon. Between January and May 2025 alone, 21 documented attacks targeted government digital infrastructure [1], many of which propagated across interconnected systems and caused prolonged service outages.

This paper focuses on the authoritative Domain Name System (DNS) infrastructure that is especially critical as it is the exclusive mechanism for mapping a service's domain names to the IP address of its hosting server instance. If this infrastructure becomes unreachable, users cannot access the service even if the website itself remains operational. If authoritative DNS records are tampered with, attackers can redirect users to fraudulent sites and harvest sensitive information. Therefore, DNS analysis has attracted significant effort (*e.g.,* [2, 3, 5]) from the measurement community.

However, evaluating authoritative DNS infrastructures remains a challenge. First, operating authoritative DNS for a domain is more complex than often assumed. Second, authoritative DNS infrastructures are often operated in a distributed manner by government-owned entities, trusted third-party local operators, or foreign (cloud) service providers. As a result, assessing DNS resilience for each government domain at scale requires integrating diverse information from multiple distributed data sources.

In this paper, we develop a **comprehensive assessment framework** that evaluates the operational resilience of authoritative DNS infrastructure for a target (*e.g.,* government) domain. Our framework models resilience across the three phases of the network operation process: hosting infrastructure placement, authoritative service configuration, and DNS record dispatch. This analysis provides infrastructure operators, domain owners, and administrative agencies with clear, quantitative, and actionable evidence to diagnose suboptimal settings that are often obscured by operational complexity. Our framework has been applied to the authoritative DNS infrastructure that supports government domain names in six representative countries, revealing valuable and previously unseen insights into their operational resilience.

2 Modeling Authoritative DNS Infrastructure

As illustrated at the bottom of Fig. 1, a user who attempts to access a website on `domain.gov.<CC>` first resolves its IP address through a recursive resolver. This resolution proceeds through a sequence of lookups as shown in steps ① – ⑤.

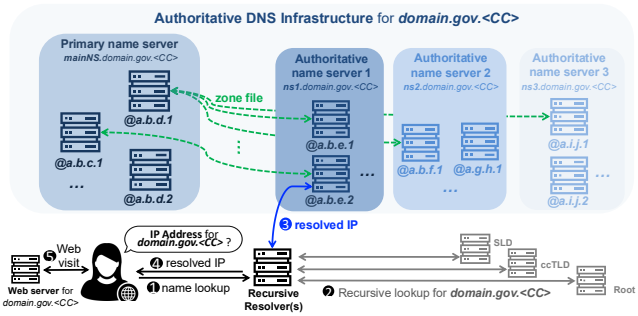


Figure 1: The authoritative DNS infrastructure for a domain.

The authoritative DNS infrastructure: Supporting step ③ requires a nontrivial authoritative DNS infrastructure operated for the domain name. As shown in the upper part of Fig. 1, this infrastructure consists of two categories of servers: the "**primary**" name server and multiple "**authoritative**" name servers. The primary name server (*e.g.,* `mainNS.domain.gov.<CC>`) hosts the source version of the DNS zone file for the domain name and may run on multiple instances, each with its own IP address (*e.g.,* `a.b.d.1`). The authoritative name servers (*e.g.,* `ns1.domain.gov.<CC>`) maintain synchronized copies of this zone file retrieved from the primary name server and are responsible for answering DNS lookup requests from users.

The network operational process: From the perspective of the government department responsible for the service, operating the authoritative DNS infrastructure involves three phases: infrastructure placement, service configuration, and DNS record dispatch. In the **infrastructure placement** phase, administrators determine where the primary and authoritative name servers will be hosted, each with a unique server name (*e.g.,* `ns1.domain.gov.<CC>`) and a corresponding physical or virtual instance. This decision includes selecting hosting organizations, choosing physical geolocations, and assigning logical IP addresses to each server instance. In the **service configuration** phase, the deployed server instances are configured to fulfill their designated roles as primary and/or authoritative name servers. From a resilience perspective, redundancy in both server types is essential. Hosting organizations must also decide whether to co-locate or separate primary and authoritative functionalities, balancing operational cost against resilience. In the DNS **record dispatch** phase, servers begin transmitting DNS data to their intended clients: the primary server synchronizes zone files with authoritative servers, and authoritative servers respond to user queries. Operators may adopt standardized security mechanisms to strengthen resilience against malicious interference, including Asynchronous Full Zone Transfer (AXFR) for controlled zone-file synchronization and DNS Security Extensions (DNSSEC) to ensure that DNS responses are cryptographically verifiable and resistant to hijacking or manipulation.

3 Resilience Assessment Methodology

Our methodology systematically collects data to describe operational practices of a domain's authoritative DNS infrastructure in each of the three phases and provides attribute-based assessment for each domain name.

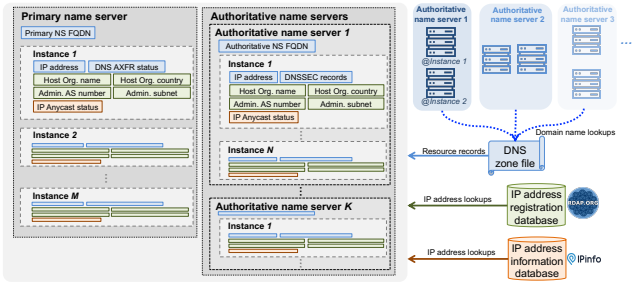


Figure 2: Our data schema for a domain.

Data schema: As illustrated on the left side of Fig. 2, the schema is organized to mirror the hierarchical structure of an authoritative DNS infrastructure. To represent resilience factors with each operational phase, the schema models the two core components of the authoritative DNS infrastructure including the primary name server and the set of authoritative name servers. Each name server is uniquely identified by its fully qualified domain name and may consist of one or more hosting instances. For every instance, the schema records its IP address, hosting organization, network configuration, and support for relevant data-security protocols. These elements appear as data components (rectangular boxes in Fig. 2) that are indexed according to their position within the hierarchy.

The values of these components are obtained from three complementary data sources, which together provide a comprehensive view of each server instance. As shown on the right side of Fig. 2, color-coded data fields correspond to the source from which each item is obtained. The process begins by querying DNS resource records from all authoritative name-server instances, retrieving information such as server roles, advertised IP addresses, and DNSSEC settings. AXFR accessibility is measured directly by issuing zone-transfer requests to all primary name-server instances from our measurement nodes. For each server instance, we retrieve administrative registration records by querying its IP address through the Registration Data Access Protocol (RDAP), which provides information on the hosting organization, subnet, and autonomous system. Some operational attributes like Anycast deployment are not exposed by the registration authorities, therefore, we supplement these records with data from the commercial IP intelligence services IPInfo, which actively tracks operational configurations and is widely used by the Internet measurement community.

In this study, we collected our dataset in November 2025 for all public-service domain names listed by federal or central governments in six representative countries including Australia, Brazil, France, Indonesia, the U.K. and the U.S., which represent diverse geographic regions and economic contexts.

Attributes and scores: We define a set of attributes each assessed with indicative scores. These scores are aggregated at four hierarchical levels of the infrastructure, allowing domain owners and administrative agencies to obtain a clear and comprehensive view of the resilience posture of the authoritative DNS infrastructure of a domain. The resilience attributes are placed at the lowest applicable hierarchical level, aligned with the operational phases, and depicted at the leftmost color-coded blocks in Fig. 3.

To enable concise and quantitative comparisons of operational practices at the executive level, we adopt a five-point Likert scale.

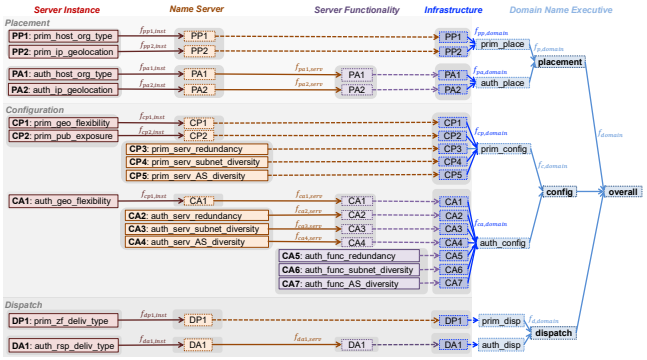


Figure 3: Attributes used to characterize the network operational resilience of an authoritative DNS infrastructure.

Each attribute in our model has at most five meaningful value options (or can be mapped to five with statistical approximation), making a larger scale unnecessary. To reduce barriers in comprehending the complex set of scores at the finest granularity, we develop impact-driven aggregation strategies that progressively combine scores of each attribute into a single attribute-level score per domain name.

The score aggregation follows the hierarchical structure indicated by the solid arrows in Fig. 3, representing how poor or strong operational practices propagate upward through the infrastructure. Drawing on industry operational practices, we observe two dominant forms of propagational impact: one in which aggregation is governed by the best available option and one in which it is governed by the worst option.

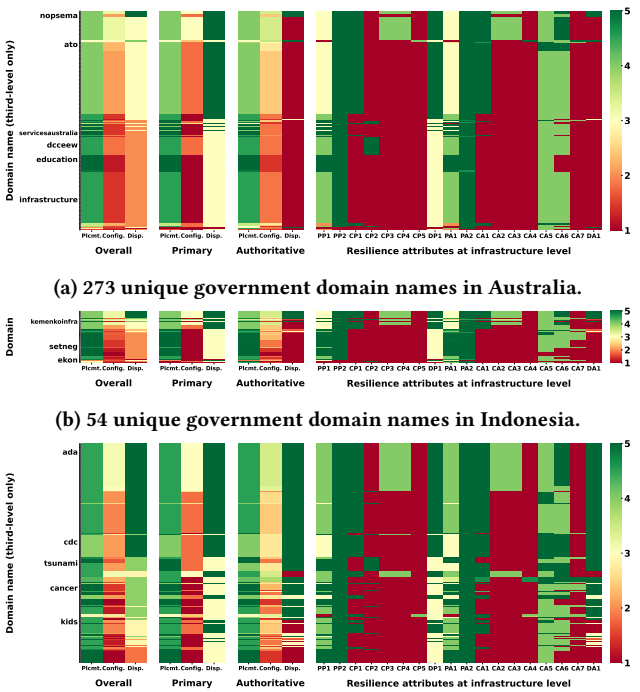
4 Assessment Results for Six Countries

We briefly summarize the assessment results and key insights obtained by applying our systematic methodology to the six representative countries. The example domain-level assessment results are provided as rows in Fig. 4, which covers the overall score per domain and their breakdown scores into three phases and individual attributes. This analysis reveals strengths and weaknesses across the three phases in operating government authoritative DNS for each country with key highlights summarized as follows.

Infrastructure placement: Indonesia and Brazil which have relatively few government domains, and France, which enforces strict national cybersecurity regulations, demonstrate stronger resilience in infrastructure placement than the U.S., U.K. and Australia, where government services more heavily rely on foreign or local cloud providers.

Service configuration: All countries show moderate configuration resilience and common weaknesses, including limited AS-level redundancy and co-hosting of primary and authoritative name servers on the same IP addresses. The U.S., U.K. and Australia demonstrate comparatively better redundancy and regional accessibility.

DNS record dispatch: The U.S. shows the strongest DNS record dispatch resilience, driven by broader DNSSEC deployment, while France shows the weakest due to low DNSSEC adoption and greater reliance on manual AXFR enforcement.



(a) 273 unique government domain names in Australia.

(b) 54 unique government domain names in Indonesia.

(c) 300 representative government domain names in the U.S.

Figure 4: Resilience heatmaps for authoritative DNS infrastructures supporting government domains. Each row corresponds to a domain name, and each column summarizes resilience scores across attributes.

5 Takeaway

We presented a systematic framework to assess the network operational resilience of authoritative DNS infrastructures supporting public-service domains operated by government agencies. Our framework is applied to government domain names published by six countries and revealed previously unknown insights into the resilience of authoritative DNS infrastructures at both the country and domain levels. Our findings demonstrate the value of a structured, data-driven approach for governance agencies seeking to understand resilience, and for domain owners to identify weaknesses and improve operational practices in their DNS configurations.

References

[1] CSIS. 2025. Significant Cyber Incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents Accessed: 2025-11-11.

[2] Rashna Kumar, Sana Asif, Elise Lee, and Fabian E. Bustamante. 2023. Each at its Own Pace: Third-Party Dependency and Centralization Around the World. *Proc. ACM Meas. Anal. Comput. Syst.* 7, 1 (March 2023).

[3] Xiang Li, Wei Xu, Baojun Liu, Mingming Zhang, Zhou Li, Jia Zhang, Deliang Chang, Xiaofeng Zheng, Chuhan Wang, Jianjun Chen, Haixin Duan, and Qi Li. 2024. TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets. In *IEEE Symposium on Security and Privacy.*

[4] Agung Septiadi, Minzhao Lyu, Hassan Habibi Gharakheili, and Vijay Sivaraman. 2026. Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services. *Proceedings of the ACM on Measurement and Analysis of Computing Systems* (Jun 2026).

[5] Donghui Yang, Zhenyu Li, Haiyang Jiang, Gareth Tyson, Hongtao Li, Gaogang Xie, and Yu Zeng. 2022. A Deep Dive into DNS Behavior and Query Failures. *Computer Networks* 214 (2022), 109131.