Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services

AGUNG SEPTIADI, University of New South Wales, Australia
MINZHAO LYU, University of New South Wales, Australia
HASSAN HABIBI GHARAKHEILI, University of New South Wales, Australia
VIJAY SIVARAMAN, University of New South Wales, Australia

Online government services, such as taxation, civil services, and immigration, are increasingly regarded as critical national infrastructure. Because these services directly influence public trust, any disruption can have significant societal and political consequences. Yet their supporting infrastructures remain vulnerable to outages from 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. While indispensable, this infrastructure also represents a potential and critical point of system failure. In this paper, we introduce a **comprehensive assessment framework** with purpose-designed mechanisms to systematically evaluate the operational resilience of authoritative DNS infrastructure supporting government services. Complementing prior studies on website hosting, recursive resolution, and DNS record integrity, our work provides a holistic view of authoritative DNS operation. Our first contribution develops a multisourced data schema that characterizes a (government) domain's authoritative DNS infrastructure across four hierarchical levels: entire hosting infrastructure, server functionality, name servers, and individual hosting instances. Using data collected from six representative countries, our second contribution identifies resilience attributes at their finest applicable hierarchy across three operational phases: infrastructure placement, service configuration, and DNS record dispatch. Our method assigns numerical scores to each attribute and aggregates them algorithmically to enable consistent and cross-domain comparisons. Lastly, we apply our method to government domains in the six countries, highlighting their strengths and weaknesses in authoritative DNS resilience and pinpointing operational practices that require improvement.

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

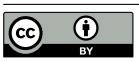
Additional Key Words and Phrases: Domain name system; DNS; network resilience

ACM Reference Format:
Agung Septiadi, Minzhao Lyu, Hassan Habibi Gharakheili, and Vijay Sivaraman. 2026. Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services. *Proc. ACM Meas. Anal. Comput. Syst.* 10, 2, Article 31 (June 2026), 30 pages. https://doi.org/10.1145/3805629

1 Introduction

Public services delivered by government agencies support essential societal functions, including taxation, healthcare, social welfare, civil service, immigration, and non-profit initiatives. As these services increasingly transition from in-person delivery to online platforms worldwide, an evolution

Corresponding author: Minzhao Lyu (minzhao.lyu@unsw.edu.au).
Authors' Contact Information: Agung Septiadi, University of New South Wales, Sydney, Australia, agung.septiadi@student.unsw.edu.au; Minzhao Lyu, University of New South Wales, Sydney, Australia, minzhao.lyu@unsw.edu.au; Hassan Habibi Gharakheili, University of New South Wales, Sydney, Australia, h.habibi@unsw.edu.au; Vijay Sivaraman, University of New South Wales, Sydney, Australia, vijay@unsw.edu.au.



ACM 2476-1249/2026/6-ART31
https://doi.org/10.1145/3805629

reflected globally in the United Nation's E-government Development Index [76], the underlying digital systems have become critical infrastructure and the focus of substantial public investment. For example, in 2025, the U.S. government allocated approximately US$75.1 billion for civilian federal information technology (IT) systems [77], and the European Union earmarked roughly €208.1 billion to advance the digital transformation across public service infrastructure [21].

Given this centrality, disruptions to government digital infrastructure 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 [13], many propagating across interconnected systems and causing prolonged service outages [63]. Australia, for example, reported an 11% annual rise in cyber incidents affecting government digital infrastructure in 2025 [1]. These disruptions arise from various causes, ranging from natural disasters that physically damage network assets to cyberattacks (by criminal or state-linked actors) that degrade access or compromise data integrity.

Among the digital systems required for government service availability, the **authoritative Domain Name System** (DNS) infrastructure is especially critical. 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, such as during the large-scale Amazon AWS DNS outage in 2025 [69], 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.

Given these risks, industry groups have long promoted operational best practices to strengthen service resilience [55], and many governments, including those of the U.S., the U.K., and Australia, fund programs aimed at improving the robustness of their digital infrastructure [2, 70, 77]. Despite these efforts, evaluating authoritative DNS infrastructures remains a challenge. First, as we will discuss in §2, operating authoritative DNS for a service domain is more complex than often assumed. Second, public-service DNS infrastructures within a country are operated in a highly distributed manner by government-owned entities, trusted third-party local operators, or foreign (cloud) service providers. As a result, assessing DNS resilience at scale requires integrating diverse information from multiple distributed data sources.

Motivated by these challenges, prior research has examined various dimensions of network resilience across infrastructure supporting (government) digital services. For example, Habib *et al.* [28] developed a statistical framework that quantifies Internet dependence using measures of centralization and regionalization across website hosting, DNS resolution, and certificate authority ecosystems, demonstrating their influence on infrastructure resilience. From a placement perspective, Kumar *et al.* [42] analyzed the organizational types, such as third-party providers or state-owned enterprises, that host government websites across countries. Geopolitical factors have also been studied, including DNS, PKI, and hosting infrastructures supporting Russian government domains [37]. Work focused specifically on DNS resilience has investigated redundancy in recursive resolution [74] and the availability of authoritative DNS records [32]. Despite previous studies on DNS resilience, a methodology that comprehensively evaluates the operational resilience of authoritative DNS infrastructure is lacking, as is the application to government services. To address the gap, we assess the network resilience of authoritative DNS infrastructure through three operational phases that have not been considered previously: infrastructure placement, service configuration, and DNS record dispatch.

In this paper, we develop a **comprehensive assessment framework** that empirically 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 phased

analysis provides infrastructure operators, domain owners, and administrative agencies with clear, quantitative, and actionable evidence to diagnose improper or suboptimal authoritative DNS settings that are often obscured by operational complexity. Coupled with an automated, multisource data-processing pipeline, our framework has been applied to the authoritative DNS infrastructure supporting government domain names across six representative countries, revealing valuable and previously unseen insights into their operational resilience. Specifically, the contributions of this paper are threefold.

Driven by our qualitative model (§2) of the three-phase network operational process for authoritative DNS infrastructure and informed by industry best practices for operational resilience, our **first** contribution (§3) captures information relevant to each phase for each element in the four hierarchical levels of authoritative DNS supporting a domain name, from infrastructure and server functionality to name servers and hosting instances. The schema is populated with data from authoritative name servers, Internet resource registries, and trusted IP intelligence sources. We automate this data collection and compile a dataset of 7,307 government services across six countries spanning diverse geographic and economic contexts. Using Australia as a representative country, we present operational practices that impact the resilience of government services.

To enable an interpretable and comparable evaluation of authoritative DNS resilience, our **second** contribution (§4) develops a systematic methodology to assess resilience per domain. We define 18 operational resilience attributes that span the three operational phases of placement, configuration, and dispatch, each mapped to its relevant hierarchy within the authoritative DNS infrastructure. Each attribute is assigned a five-point numerical score, ranging from worst to best, based on its impact on resilience and its alignment with industry-recommended practices. These scores are hierarchically aggregated using an impact-driven algorithm, producing both fine-grained visibility into operational settings and a consolidated resilience summary suitable for executive interpretation.

Our **third** contribution (§5) applies our methodology to 7,307 government domain names in six countries (Australia, Brazil, France, Indonesia, the U.K., and the U.S.), allowing a cross-national assessment of authoritative DNS operational resilience. Comparative analysis reveals unique national patterns in the three phases (placement, configuration, and dispatch) shaped by differing infrastructure strategies and policy environments. For example, Australia and the U.K. rely heavily on foreign cloud providers even for primary authoritative functionality; France and Indonesia demonstrate strong placement resilience due to local hosting policies, but exhibit lower resilience in service configuration and DNS record dispatch; and the U.S. government domains generally score well overall, yet exhibit some weaknesses such as exposure of primary name servers to the public Internet, insufficient subnet redundancy, and not recommended DNSSEC algorithms. These findings demonstrate that our assessment framework provides actionable insights for both DNS operators and government agencies, enabling them to systematically benchmark their current practices and strengthen operational resilience to better serve their citizens.

2 Preliminary on Network Operation of Authoritative DNS Infrastructure

In this section, we introduce the three-phase network operation process that governs the authoritative DNS infrastructure of a given domain name (§2.1) and summarize industry-recommended practices that strengthen operational resilience across these phases (§2.2).

2.1 Authoritative DNS Infrastructure of (Government) Domain Names

The authoritative DNS infrastructure is the sole authority responsible for mapping a domain name to the IP address(es) of the service that hosts it. 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

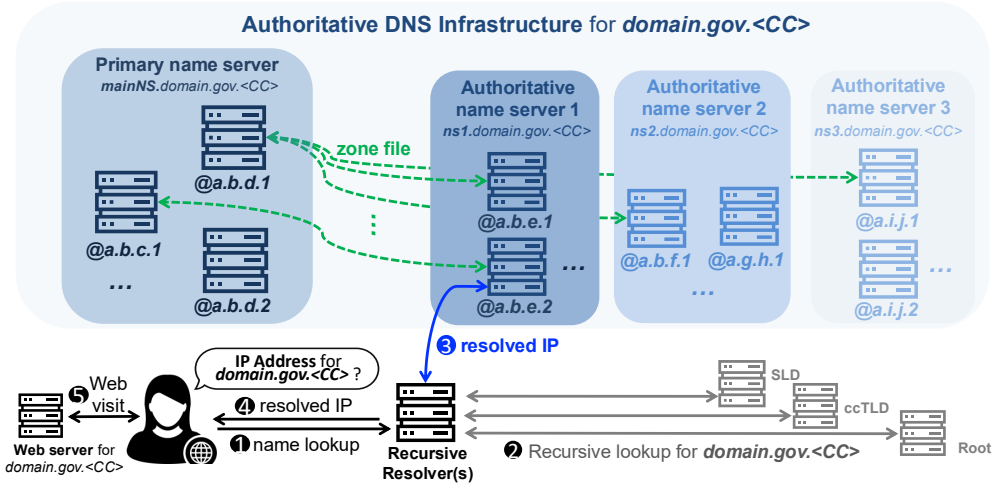


Fig. 1. A simplified view of the authoritative DNS infrastructure for a domain and its role in resolving and serving user web requests.

resolver. This resolution proceeds through a sequence of lookups, from the root, to the country code top-level domain (ccTLD), and then to the second-level domain (SLD), as shown in steps ① and ②. The process continues until the resolver reaches an authoritative name server instance on the IP address `a.b.e.2` corresponding to `ns1.domain.gov.<CC>` in step ③. This server instance hosts a copy of DNS records (*i.e.,* zone file) for the requested domain. Once the recursive resolver obtains the IP address of the web server hosting `domain.gov.<CC>` (step ④), the user's browser connects to the service in ⑤.

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. As studied in prior work [28], 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 [75], 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) [44] for controlled zone-file synchronization and DNS Security Extensions (DNSSEC) to ensure that DNS responses are cryptographically verifiable and resistant to hijacking or manipulation.

2.2 Industry Best Practices for Resilient Operation of Authoritative DNS Infrastructure

Having outlined the three phases of the network operational process for authoritative DNS infrastructure, we now summarize industry-recommended practices that enhance resilience against physical disruptions, such as natural disasters and power outages [56], and network-based threats, such as IP- or DNS-layer DDoS attacks [30] and integrity-compromising exploits [29]. Adopting these practices typically increases infrastructure cost and operational complexity, but significantly strengthens service robustness.

From the perspective of **infrastructure placement**, the Internet community recommends [28] that organizations hosting authoritative DNS servers and their instances maintain a close administrative relationship with the responsible government department, such as through State-Owned Enterprises (SOE). Hosting on reputable international cloud providers (*e.g.,* Amazon AWS) or trusted domestic providers is also considered acceptable. In contrast, hosting DNS infrastructure on small, foreign-operated enterprises or on entities lacking formal registration poses substantial resilience risks. Physical placement also matters: for government services primarily accessed by local residents, both primary and authoritative DNS instances should ideally be hosted within the country with locally registered/operated IP addresses to ensure administrative proximity and reduce exposure to geopolitical disruptions.

During the **service configuration** phase, best practices articulated in standards such as RFC 2182 [64] emphasize shielding the primary DNS function from public exposure and ensuring sufficient redundancy across both primary and authoritative roles. The primary name server should only be reachable by trusted authoritative servers and should not be co-hosted with publicly exposed authoritative functionality. Redundancy can be achieved by enabling IP Anycast [47] for the primary service so that authoritative servers connect to the nearest available instance. If Anycast is not used, the primary service should operate on multiple instances, preferably more than two, each with a unique IP address and located in different autonomous systems (ASes) or subnets. Authoritative DNS functions should likewise employ multiple server names (*e.g.,* {`ns1, ns2, ns3`}`.domain.gov.<CC>` in Fig. 1), each implemented using Anycast or backed by multiple IP addresses.

Finally, in the **record dispatch** phase, which includes zone-file transfers from the primary server to authoritative servers and DNS responses served to clients, standardized security mechanisms should be enforced to defend against integrity and hijacking attacks. Specifically, Asynchronous Full Zone Transfer (AXFR) should be used to distribute zone files only to trusted authoritative servers securely, and DNS Security Extensions (DNSSEC) should be enabled to ensure that DNS responses are cryptographically verifiable, as discussed earlier in §2.1.

3 Analyzing Authoritative DNS Resilience with Multisourced Data Schema

Building on the three-phase operational model of authoritative DNS infrastructure and the associated industry best practices, this section introduces our multisourced data schema that characterizes the network operational resilience of a domain name (§3.1). We then describe the collection of a large-scale dataset covering government-listed public service names in six countries (§3.2), followed by an illustrative analysis using one representative medium-sized country as a case study (§3.3).

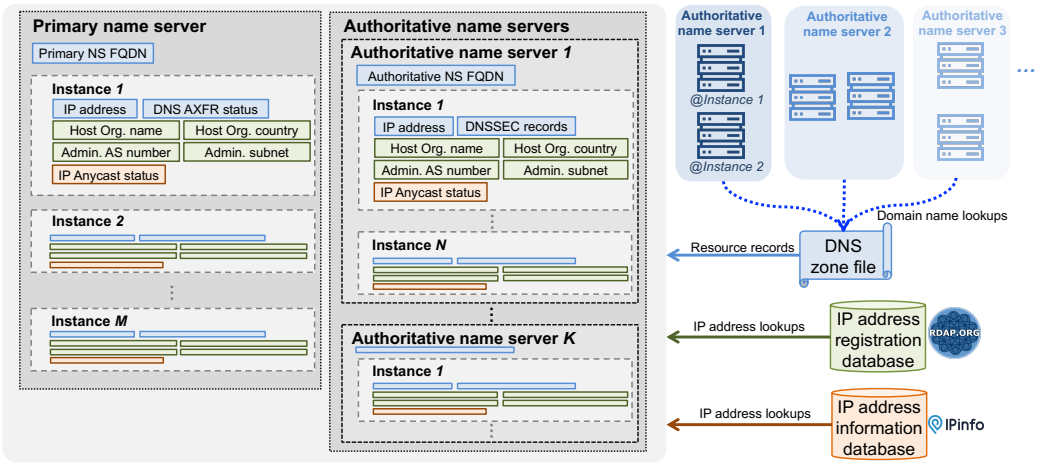


Fig. 2. Our structured **data schema** (the left region in gray) integrating DNS resource records, IP registration data, and IP operational information to represent the resilience-relevant attributes of authoritative DNS infrastructure for a government domain.

3.1 Structured Data Schema for a (Government) Domain Name

To fully capture the network resilience of the authoritative DNS infrastructure for a domain name, we design a data schema that aggregates operational information that reflects the practices across the three phases of infrastructure placement, service configuration, and DNS record dispatch. As illustrated on the left side of Fig. 2, the schema is organized to mirror the hierarchical structure of an authoritative DNS infrastructure. It is populated through automated scripts that query three distinct categories of data sources.

To represent resilience factors with each operational phase (§2), the schema models the two core components of the authoritative DNS infrastructure: the primary name server and the set of authoritative name servers. Each name server is uniquely identified by its fully qualified domain name (*i.e.,* `Primary NS FQDN` and `Authoritative NS FQDN`) 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. Next, for each server instance, we retrieve administrative registration records by querying its IP address through the Registration Data Access Protocol (RDAP) [68], which provides information on the hosting organization, subnet assignment, and autonomous system. Since some operational attributes, like Anycast deployment, are not exposed by the registration authorities, we supplement these records with data from the commercial IP

intelligence services IPInfo [33], which actively tracks operational configurations and is widely used by the Internet measurement studies [27, 42, 62, 79, 85].

The complete schema is represented in JSON format, with each data component indexed within the hierarchical structure. For each domain name, the data collection module generates a single JSON object by integrating the three data sources, which is then processed by the resilience assessment module. Details of the measurement setup and processing pipeline are provided in Appendix §B.

As underlying data sources, we assume that IP registration information obtained via the Registration Data Access Protocol (RDAP), standardized by the Internet Engineering Task Force (IETF), is sufficiently accurate for identifying infrastructure ownership. We also use the IPInfo database as the sole source to determine IP Anycast status. While alternative IP intelligence databases could be used for validation or substitution, exploring such extensions is beyond the scope of this study, which focuses on the resilience modeling schema and assessment methodology.

We further note that our proposed schema can be extended. In its current form, it captures the categorical characteristics of hosting infrastructure, such as hosting organization type and binary geolocation (*i.e.,* internal or external to the respective country). Additional dimensions, such as concentration across cloud providers or finer-grained geolocation, could support more detailed modeling.

3.2 Dataset Collection for Government-Listed Public Service Domains at National Scale

We collected our dataset in November 2025 to assess all public-service domain names listed by federal or central governments in six representative countries. The six countries represent diverse geographic regions (North America, Europe, and Asia-Pacific) and economic contexts (developed and developing economies). In addition, their government agencies maintain public services domain lists in English, ensuring accessibility and consistency of records for measurement.

Table 1 summarizes these countries, the government authorities responsible for publishing the official service lists, the total number of listed public-service domains, and the number of unique parent domain names, each supported by a distinct authoritative DNS infrastructure. By comparing the number of fully qualified domain names (*e.g.,* `www.ready.gov`) with the number of unique parent domains (*e.g.,* `ready.gov`), we observe three distinct operational strategies for authoritative DNS used at the government level in the six countries.

Table 1. Summary of government-listed public-service domains and the corresponding unique parent domain names for each of the six studied countries.

Country	Authority	# services	# parent domains
AU	`finance.gov.au` [2]	790	273
BR	`gov.br` [9]	41	2
FR	`data.gouv.fr` [16]	659	192
ID	`setkab.go.id` [71]	60	54
UK	`gov.uk` [26]	5,548	5,475
US	`get.gov` [14]	1,349	1,308

The **first** strategy, used by the U.S., the U.K., and Indonesia, assigns a dedicated domain name to nearly every online public-service endpoint, with only a small number of services sharing the same domain. This decentralized model offers individual government departments substantial flexibility in managing the authoritative DNS infrastructures that support their respective services. The **second** strategy, adopted by Australia and France, groups multiple services under a small set of shared parent domains, typically two or three services per domain, often reflecting departmental structure. For example, both `consult.treasury.gov.au` and `ttaasag.treasury.gov.au` fall under the parent domain `treasury.gov.au` for the Department of Treasury. Brazil represents the **third** strategy, in which authoritative DNS operations are highly centralized. All 41 listed public-service domains map to only two parent domains `bcb.gov.br` and `www.gov.br`.

For every domain name identified across the six countries, we collected the full set of data components defined by our schema in §3.1. These data support the manual analysis presented in §3.3 and form the basis of our systematic resilience assessment in §4. As we show later, the resulting assessments reveal distinct resilience profiles across countries that correlate strongly with their administrative structures and the operational strategies adopted for authoritative DNS infrastructure.

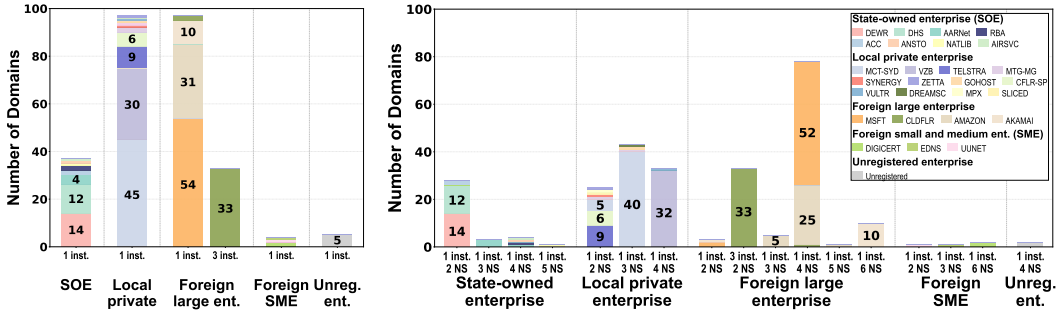
3.3 Analytical Insights for a Medium-Sized Country

Analysis of our dataset reveals a wide variety of network operational practices within authoritative DNS infrastructures supporting government services, with implications for resilience in terms of diversity and complexity. To illustrate these characteristics, we present selected observations for Australia. Australia represents a medium-sized authoritative DNS infrastructure for government services, with moderate complexity in placement, configuration and dispatch practices. This makes it a suitable illustrative case to motivate the resilience modeling and assessment methods introduced in §4.

3.3.1 Infrastructure placement. We begin by examining the two fields in our data schema that reflect infrastructure for each domain name: the "host Org. name" and the "hosting country", which together indicate the administrative ownership and physical location of each primary or authoritative name-server instance. Host organizations fall broadly into four categories, State-Owned enterprises (SOE), local private enterprises, foreign large enterprises, and foreign small-and-medium (SME) enterprises, each associated with varying levels of operational resilience [42]. In addition, a small number of instances appear with incomplete registration records; these are classified as "unregistered", representing the least trustworthy category.

Primary name servers by enterprise category: For the primary name server, which serves as the sole authoritative source for a domain's zone file, instances are deployed on one or three physical or virtual servers, each assigned a unique IP address. Fig. 3a shows the number of domain names whose primary name servers are hosted in each enterprise category, with stacked bars indicating the number of hosting instances and segmented by unique hosting organization. Among the 273 government-listed service domains, 37 (13.55%) have their primary name servers directly operated by 8 SOEs, typically considered the most resilient arrangement. However, all SOE-hosted primary servers run on a single instance, reducing resilience from a service-configuration standpoint. These observations motivate the definition of resilience attributes that capture enterprise types and the number of hosting instances in §4.

A further 97 domains (35.53%) operate their primary name server on a single instance hosted by local private enterprises, offering reasonable resilience against foreign influence [36]. Another 97 domains (35.53%) rely on large international cloud providers, including Microsoft, Cloudflare, Amazon, Google, or Akamai, for their primary DNS hosting, while 33 domains (12.09%) use Cloudflare across three instances. As will be discussed later in §3.3.2 and §3.3.3, hosting on major cloud platforms generally improves resilience in the configuration and dispatch phases. However, these providers are foreign entities, raising concerns about digital sovereignty. A small number of domains (4, 1.47%) use foreign SMEs to host their primary name servers, a configuration that introduces substantial operational risks for such a critical function. The worst cases involve five domains (1.83%) whose primary servers are hosted on instances without complete registration information; notably, these domains also co-host their authoritative name servers on the same instance, thereby exposing primary functionality, intended to remain shielded from public access, to unnecessary cyber risk.



(a) Primary name servers. (b) Authoritative name servers.

Fig. 3. Hosting-organization categories for (a) primary and (b) authoritative name servers supporting government-listed domain names in Australia. Each server may run on one or more hosting instances. Hosting enterprises are grouped into five categories: state-owned enterprises (SOE), local private enterprises, foreign large enterprises, foreign SMEs, and unregistered entities, with different implications for resilience.

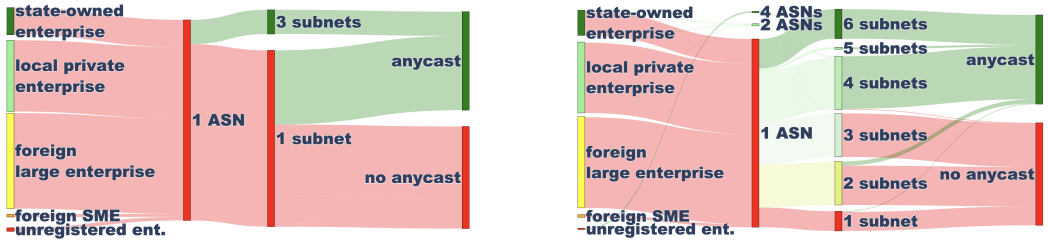
Authoritative name servers by enterprise category: Unlike the sole primary name server required to maintain a consistent zone-file origin, each domain typically advertises multiple authoritative name servers (*e.g.,* two to six in this country, as shown by the "auth" x-ticks in Fig. 3b) to improve regional (and global) accessibility. Each authoritative server is itself hosted on one or three instances, though different patterns appear in other countries. For example, the authoritative server `aliza.ns.cloudflare.com` for `aifs.gov.au` operates across three distinct IP addresses.

The combination of multiple authoritative servers, each with multiple hosting instances, introduces significantly more complexity than the configuration of a single primary server on multiple instances. In this country, 270 domains (98.90%) have all authoritative instances hosted by a single enterprise category, while 3 domains (1.10%) distribute their authoritative hosting across two categories. We show a simplified count of domain names in Fig. 3b summarizing the dominant enterprise type for authoritative hosting per domain. It can be seen that most domains rely primarily on foreign large enterprises (47.62%), followed by local private enterprises (37.00%) and SOEs (13.19%). A small number of domains depend on foreign SMEs for authoritative hosting, representing the least resilient placement.

3.3.2 Service configuration. In the service-configuration phase, each hosting instance (whether it supports the primary or authoritative name server) is configured to control how it is reached by Internet users. To understand how practices in this phase affect network resilience, we analyze the `IP address`, `Admin. subnet`, `Admin. AS number`, and `IP Anycast status` fields in our data schema, which together describe the network address (IP) configuration of each server instance. Redundancy in both name servers and hosting instances, already discussed in §3.3.1, also plays a central role in this phase.

Primary name servers by the hosting redundancy: Overall, redundancy remains limited for most government domain names in this country. As shown in Fig. 3a and Fig. 3b, 240 domains (87.91%) host their primary name servers on single instances, and 57 domains (20.88%) advertise only two authoritative name servers, each deployed on a single instance. Such configurations offer little protection against localized failures or targeted network attacks.

By contrast, the 33 domains whose primary name servers span three instances, all rely on cloud providers (specifically, Cloudflare) that configure these instances using Anycast routing [47]. Anycast enables user requests to reach the nearest Cloudflare node, providing strong resilience against network failures and geographically distributed attacks. However, this contrasts with the 37



(a) Primary name servers. (b) Authoritative name servers.

Fig. 4. Overview of operational practices in (a) primary and (b) authoritative name servers of Australian government public-service domains. Hosting-enterprise types, administrative ASN and subnet diversity, and Anycast configurations vary substantially across domains, leading to differing resilience profiles.

domains (13.55%) whose primary name servers are operated by State-Owned Enterprises. While SOE operations offer resilience against geopolitical and jurisdictional risks, all of these instances reside within a single administrative subnet, and none use Anycast, significantly limiting flexibility and redundancy in access paths. The relationship among enterprise type, administrative subnet/ASN diversity, and Anycast use for primary servers is shown in Fig. 4a. Similar patterns hold for domains whose primary servers are hosted by local private enterprises: 96 out of 97 domains are placed within a single subnet without Anycast, with one exception `aafcans.gov.au` using Anycast across a single subnet. In §4, we will define resilience attributes that capture hosting redundancy and access flexibility to characterize these service configuration practices.

Authoritative name servers by the hosting redundancy: The configuration of authoritative name servers is even more complex, as illustrated in Fig. 4b. The interplay among hosting-organization type, addressing configuration, subnet/ASN diversity, and Anycast deployment varies widely across domains, highlighting the need for a systematic, multi-attribute resilience assessment, far beyond what single-aspect analysis in prior work typically capture [75].

3.3.3 DNS Record Dispatch. In the record-dispatch phase, we examine the two fields in our data schema (*i.e.,* `AXFR status` and `DNSSEC records`) that indicate whether secure protocols are enforced to protect DNS record integrity. AXFR governs the transfer of zone files from the primary name server to authoritative servers, while DNSSEC protects responses served by authoritative servers to Internet users.

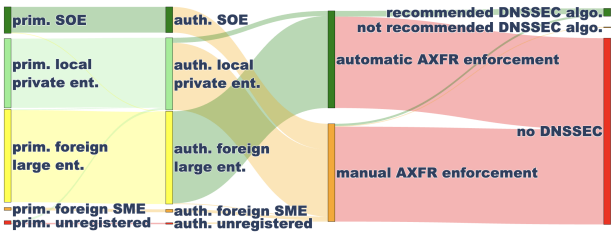


Fig. 5. Operational practices in the DNS record-dispatch phase for Australian government public-service domains, showing the relationship between primary-server hosting enterprise type, AXFR enforcement method, and the worst-case DNSSEC configuration among authoritative server instances.

Dispatching from the primary to authoritative name servers: For the primary name servers of government domains in this country, **restricted distribution** of zone files via AXFR is consistently enforced: only authorized authoritative server instances are permitted to fetch zone data. As shown in Fig. 5, this enforcement is automatic for 136 domains (49.82%), all of which rely on specialized managed DNS services provided by Google, Akamai, and Cloudflare [4, 12, 25]. The remaining 137 domains (50.18%) use manual (*i.e.,* not managed DNS services) AXFR configuration by IT operators, a practice that carries a higher risk of misconfiguration [38]. In particular, in all six

countries studied, every public-service domain enforces AXFR on its primary servers, which is captured as a resilience attribute in the systematic assessment in §4.

Dispatching from authoritative servers to clients: However, DNSSEC deployment shows substantial variation between hosting-enterprise categories. As also shown in Fig. 5, none of the 37 domains (13.55%) operated by State-Owned Enterprises enforce DNSSEC on their authoritative servers, and all rely on manually configured AXFR. Among the 97 domains (35.53%) managed by local private enterprises, 90 (32.97%) also use manual AXFR and do not deploy DNSSEC. A small subset of six defense-service domains uses automatically enforced AXFR but likewise omits DNSSEC. One domain uses standard zone file delivery and deploys DNSSEC, but with cryptographic algorithms that do not meet IETF recommendations [78]. In contrast, 130 domains (47.62%) managed by foreign large enterprises rely on automatic AXFR enforcement, reflecting mature operational practices, yet only 8 domains (2.93%) in this group deploy DNSSEC, all of which use recommended algorithms. This highlights an operational gap: while zone-transfer protection is widely implemented, DNSSEC adoption remains limited even among domains hosted by technically sophisticated providers.

4 Systematic Assessment of Authoritative DNS Resilience for a Domain Name

Building on the comprehensiveness of our data schema and the complexity revealed in the preceding analysis, we now develop a systematic assessment methodology for authoritative DNS resilience. Our approach defines a set of descriptive attributes (§4.1) and converts them into comparable indicative scores for each domain's authoritative DNS infrastructure (§4.2). These scores are aggregated at four hierarchical levels of the infrastructure (§4.3), allowing domain owners and administrative agencies to obtain a clear and comprehensive view of the resilience posture of the authoritative DNS system of a government domain.

4.1 Attributes for Authoritative DNS Resilience at their Lowest Hierarchical Levels

As discussed in §2.1, the authoritative DNS infrastructure for a domain name can be viewed at four hierarchical levels: the overall infrastructure, the two name-server functionalities (primary or authoritative), the name servers themselves, and their hosting instances. As shown in §2.2 and empirically illustrated in §3.3, placement and configuration decisions at any of these levels can materially affect the operational resilience of the entire infrastructure. To capture these effects, we define resilience attributes at the lowest applicable hierarchical level, aligned with the operational phases, and depicted at the leftmost color-coded blocks in Fig. 6.

4.1.1 Placement of Authoritative DNS Infrastructure. For the infrastructure placement phase, we define four attributes, namely "prim_host_org_type", "prim_ip_geolocation", "auth_host_org_type", and "auth_ip_geolocation", abbreviated as `PP1`, `PP2`, `PA1`, and `PA2`, that describe the hosting enterprise type and the IP geolocation for primary and authoritative name-server instances.

Based on our observations in §3.3.1, the hosting enterprise attributes `PP1` and `PA1` take one of five values: "state-owned enterprise", "local private enterprise", "foreign large enterprise", "foreign small-and-medium enterprise", and "unregistered enterprise". These categories imply different levels of resilience with respect to geopolitical stability and administrative control.

For geolocation attributes `PP2` and `PA2`, we use two-letter country codes derived from the IPInfo geolocation database [33]. Noting that Anycast-enabled IP addresses operated by international cloud providers may appear with foreign registration information (*i.e.,* the "Host Org. country" field) but serve clients locally; in such cases, the local country code is assigned to reflect their operational geography. In our implementation (Appendix §B), `PP2` and `PA2` are derived by mapping the "Host Org. name" field of each server instance to an enterprise-classification catalog maintained for each studied country.

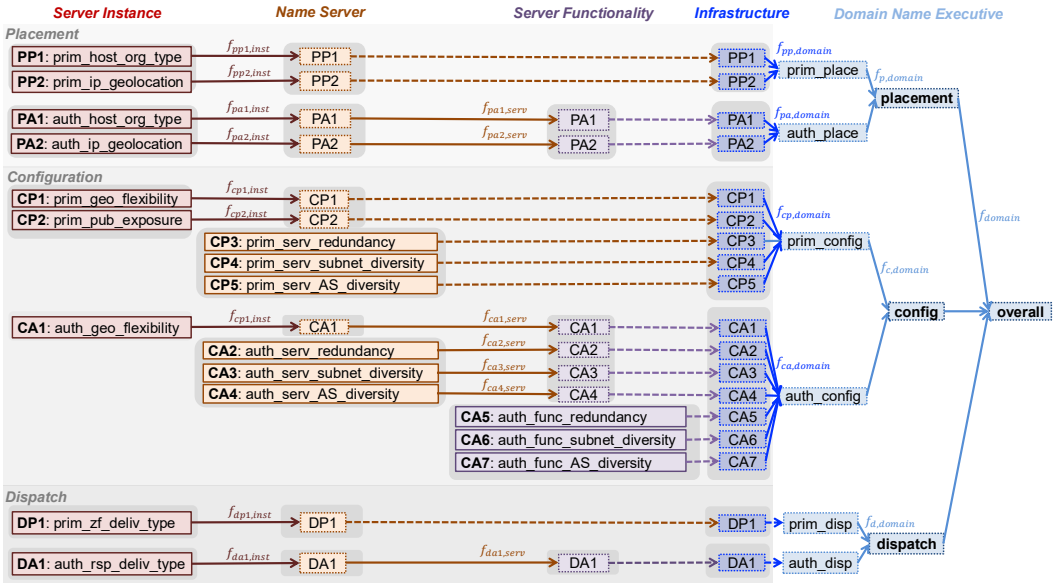


Fig. 6. Attributes used to characterize the network operational resilience of an authoritative DNS infrastructure, organized at four hierarchical levels (server instance, name server, server functionality, and overall infrastructure), as outlined in the gray region.

4.1.2 Configuration of Name Server Functionalities. In the middle block of Fig. 6, we define twelve attributes describing configuration practices that impact resilience during the service configuration phase. The first five attributes `CP1–5` apply to the primary name server, and the remaining seven `CA1–7` describe the authoritative name servers.

For primary-server instances, `CP1` ("prim_accessibility") indicates whether Anycast is enabled, providing geographic flexibility and improved fault tolerance. `CP2` ("prim_pub_exposure") indicates whether the primary instance is co-hosted with authoritative functionality, a practice that increases exposure to public-facing threats. Attributes `CP3–5`, defined at the name-server level, capture redundancy and diversity: the number of IP addresses configured with primary functionality, the diversity of hosting subnets, and the diversity of autonomous systems (ASes).

Analogous attributes are defined for authoritative name servers: `CA1` reflects regional accessibility through Anycast usage at each instance, `CA2` captures redundancy at the authoritative name-server level, and `CA3` and `CA4` measure subnet and AS redundancy per authoritative server, and `CA5` captures redundancy in authoritative functionality (*i.e.,* the number of distinct authoritative server names such as `ns1.gov.com.<CC>`). Finally, `CA6` and `CA7` describe the redundancy of authoritative servers on different subnets and ASes, respectively.

4.1.3 Dispatch of Authoritative DNS Records. For the record-dispatch phase, we define two attributes: `DP1` and `DA1` to capture the enforcement of secure protocols governing zone-file delivery and DNS-response integrity.

`DP1` ("prim_zf_deliv_type") describes how AXFR is enforced for distributing DNS zone files from the primary server instance to authorized authoritative servers. As discussed in §3.3, the attribute takes one of three values: "automatic cloud-based enforcement", "manual enforcement", or "no enforcement". This classification is determined by comparing the hosting enterprise with our maintained list of cloud DNS providers known to automatically enforce AXFR, along with the AXFR-status field in the data schema.

DA1 ("auth_rsp_deliv_type") describes DNSSEC deployment on authoritative name server instances and takes one of three values: "recommended algorithms", "not recommended algorithms", and "not configured". These values indicate whether DNSSEC is enabled and, if so, whether cryptographic algorithms comply with the IETF recommendations [78]. In our processing pipeline (Appendix §B), DA1 is assigned by comparing the algorithms listed in each DNSSEC record with the recommended-algorithm set.

4.2 Assessment Scores for Each Attribute

Having defined a comprehensive set of attributes and possible values that describe authoritative DNS operational practices for government domains, we now introduce a quantitative scoring scheme to evaluate each attribute. We adopt a five-point Likert scale [54], which is widely used in scoring frameworks across disciplines [20, 43]. Each attribute in our model has at most five meaningful value options (or can be mapped to five), making a larger scale unnecessary.

Our primary motivation for assigning a Likert score to each attribute is to enable concise and quantitative comparison of operational practices at the executive level. These scores serve as as a diagnostic heuristic, allowing managerial and policy stakeholders to interpret resilience landscape through simplified numerical indicators. Each score corresponds to a specific operational practice and retains an interpretable meaning for detailed analysis. These scores are not intended for direct comparison across attributes, as each attribute reflects a distinct operational context and may vary across assessors.

Appendix Table 2 presents the assessment criteria for the attributes at their lowest hierarchical levels (instance, name server, or name server functionality). Each attribute describes one aspect of the operational resilience for primary or authoritative DNS functionality. As discussed intuitively in §3.3, these attribute values impact resilience in different ways. We formalize this by assigning each attribute option a score from 1 to 5, where 1 represents the least resilient practice and 5 represents the most resilient one. This enables both comparative analysis across domains and meaningful aggregation to higher hierarchical levels.

Attributes with five finite value options: Attributes PP1 and PA1, which describe the hosting-enterprise type for primary and/or authoritative server instances, each have five finite options. These options are scored from five (most resilient, *e.g.,* state-owned enterprise) to one (least resilient, *e.g.,* an unregistered entity in the IP registry).

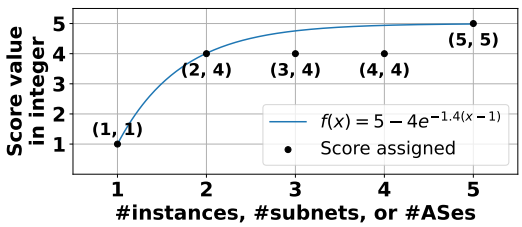


Fig. 7. Exponential saturation function used to assign scores for redundancy/diversity attributes, capturing diminishing resilience returns as the number of instances, subnets, or ASes increases. The function is constrained by the minimum score (1,**1**) and the recommended operational practice (2,**4**).

Attributes with three finite value options: For DNS record dispatch-phase attributes DP1 and DA1, each takes one of three options: strong and recommended enforcement of data-integrity mechanisms, insufficient enforcement (*e.g.,* manual AXFR configuration for DP1 and weak DNSSEC algorithms for DA1), and no enforcement. These are mapped to scores 5, 3, and 1, respectively.

Attributes with two finite value options: Five attributes, PP2, PA2, CP1, CP2, and CA1, have binary values that clearly reflect good or poor resilience practices. Therefore, these are assigned a value of 1 or 5. For example, CP2 indicates whether a primary server instance shares its IP address with an authoritative name server instance. Co-location reduces operational costs but exposes the primary instance to the same risks

as the publicly reachable authoritative server. Thus, co-location is scored 1 (worst practice), whereas using a dedicated IP address is scored 5 (best practice).

Attributes with infinite value options: Nine attributes (*i.e.,* `CP3-5` and `CA2-7`) describe the counts of server instances, name servers, subnets, or ASes, and therefore have theoretically unbounded value ranges. For example, the attribute `CP3` represents the number of hosting instances for the primary name server. Although an extremely large number of instances would maximize redundancy, operational experience shows diminishing returns, with most DNS operators recommending **two** instances/subnets/ASes as the practical and cost-effective standard for resilience [3, 11, 64]. Therefore, a value of 1 (no redundancy/diversity) is assigned 1 out of 5, and a value of 2 is assigned 4 out of 5, representing recommended best practice.

To determine a realistic threshold for full scoring, we apply a bounded exponential growth function [8], commonly used to model diminishing returns, where outputs are constrained by the minimum and maximum values in our scoring scheme. The fitted curve is shown in Fig. 7. It can be seen that the function approaches the maximum score of 5 as soon as the attribute value reaches five. Consequently, in our scoring scheme, these seven attributes receive: a full 5/5 score when the count of instances/subnets/ASes is five or more, or a score of 4/5 for values from 2 to 4.

4.3 Aggregating Scores for Comparative Assessment Across Domain Names

While attribute scores defined at their finest applicable hierarchy provide detailed visibility into operational practices, comparing resilience across domain names remains challenging because authoritative DNS infrastructures vary in their hierarchical complexity. To address this, we develop impact-driven aggregation strategies that combine scores of **each attribute** from lower levels (*i.e.,* server instance, name server, or NS functionality) into a single attribute-level score at the infrastructure level (the blue boxes in Fig. 6). Such aggregations beyond attribute-level scores provide a higher-level summary of operational resilience for a given domain name. This reduces the effort and technical expertise required to assess overall resilience, supporting initial scoping and subsequent drill-down analysis by domain operators and policy makers.

Aggregation follows the hierarchical structure indicated by the solid arrows in Fig. 6, 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 (§4.3.1) and one in which it is governed by the worst option (§4.3.2). These cases collectively form the basis of our aggregation strategies, formalized in Algorithm 1.

Some attributes do not require aggregation at specific levels because they inherently produce a single score, *e.g.,* `PP1` at the name server level. These are directly mapped to the higher level, as shown by the dashed arrows in Fig. 6.

After attribute-level scores are obtained at the authoritative DNS infrastructure level, they can be further summarized into phase-level scores. For example, $f_{pp,domain}$ and $f_{pa,domain}$ for the primary and authoritative placement attributes, and $f_{cp,config}$ and $f_{ca,config}$ for the configuration attributes. These phase-level scores are then aggregated into three operational-phase summaries: $f_{p,domain}$ for infrastructure placement, $f_{c,domain}$ for service configuration, and $f_{d,domain}$ for DNS record dispatch. The weighting of attributes and phases is inherently subjective and depends on assessor priorities. In our evaluation (§5), we adopt equal weighting across all attributes at the infrastructure-level and throughout all phases, using simple averaging to maintain interpretability and comparability. These weights represent the relative importance assigned to each attribute-level score in assessing the overall resilience of an authoritative DNS infrastructure (the "Domain Name Executive" region in Fig. 6). Therefore, they are inherently subjective and may vary across assessors, potentially resulting in different overall scores.

Algorithm 1: Aggregation of resilience scores for an attribute to the next hierarchical level using ***impact-driven strategies*** dominated by either the best or the worst score.

(1) **Input:** $\mathbf{s}_{a,h,n} \leftarrow$ the resilient scores of the attribute a for **all** items at the hierarchical level h, which belongs to the nth item at the upper $h+1$ level; $\Delta D \leftarrow$ value step; *BestStrategy* $\leftarrow$ boolean for adopting a strategy dominated by the best or the worst score;
(2) **Output:** $s_{a,h+1,n} \leftarrow$ the resilient score for the attribute a of the nth item at the hierarchical level $h+1$;
// best-score dominant strategy by decreasing the highest score with small factors.
(4) **if** *BestStrategy is true* **then**
(5) $s_{a,h+1,n,base} \leftarrow max(\mathbf{s}_{a,h,n}); s_{a,h+1,n,tmp} \leftarrow max(\mathbf{s}_{a,h,n})$;
// counting the numbers of each score value in the decreasing order.
(6) **scoreVal,scoreCt** $\leftarrow counting_{\downarrow,1}(\mathbf{s}_{a,h,n})$;
(7) **for** val, ct *in* ***scoreVal,scoreCt*** **do**
(8) **if** val *is* ***not*** $s_{a,h+1,n,base}$ **then**
// decrease from the highest score.
(9) $s_{a,h+1,n,tmp} \leftarrow s_{a,h+1,n,tmp} - (ct * \Delta D / \sum(\mathbf{scoreCt}))^{val}$;
// worst-score dominant strategy by increasing the lowest score with small factors.
(11) **if** *BestStrategy is false* **then**
(12) $s_{a,h+1,n,base} \leftarrow min(\mathbf{s}_{a,h,n}); s_{a,h+1,n,tmp} \leftarrow min(\mathbf{s}_{a,h,n})$;
// counting the numbers of each score value in increasing order.
(13) **scoreVal,scoreCt** $\leftarrow counting_{\uparrow,1}(\mathbf{s}_{a,h,n})$;
(14) **for** val, ct *in* ***scoreVal,scoreCt*** **do**
(15) **if** val *is* ***not*** $s_{a,h+1,n,base}$ **then**
// increase from the lowest score.
(16) $s_{a,h+1,n,tmp} \leftarrow s_{a,h+1,n,tmp} + (ct * \Delta D / \sum(\mathbf{scoreCt}))^{(6-val)}$;
(17) **return** $s_{a,h+1,n} \leftarrow s_{a,h+1,n,tmp}$;

4.3.1 Aggregating scores dominated by the best case. Eight attributes, including `PA1-2`, `CP1`, and `CA1-4`, exhibit propagational behavior in which overall resilience is governed primarily by the best operational practices. Consider `PA1`, which describes the type of hosting company for an authoritative name-server instance. Authoritative servers do not edit or originate DNS records; they only serve users with a copy of the records. Thus, having at least one instance operated by a highly trusted enterprise (*e.g.,* an SOE) can preserve service availability even if other instances are hosted by less trustworthy entities. In such cases, the presence of a highly resilient instance dominates the overall resilience of the authoritative name server.

Consequently, when aggregating instance-level scores into a single score for the authoritative name server, the aggregated value should remain the best score and should never fall below the next-lower resilience level. For example, if all instances are operated by SOEs (each scoring 5), then the aggregated score is unequivocally 5. If one instance scores 5 and the remaining instances score 1, the aggregate score will be $(4, 5]$, convergent to 4 as the number of poorly configured instances increases. The score cannot fall below 4, because a configuration that includes one instance operated by a state-owned enterprise (SOE) is inherently more resilient than a configuration where all instances are hosted by local private enterprises (which score 4). This reflects the realistic operational difficulty of remediating a large number of poorly configured instances while still benefiting from the uplift provided by a highly resilient one.

To algorithmically capture this behavior, we develop a best-score-dominant aggregation strategy, in the first block in Algorithm 1 (lines #4-12). As shown in line #9, for each unique score value val

that is lower than the best value $s_{a,h+1,base}$ in the set, the aggregated score is reduced by a fractional exponent $\left(ct * \Delta D / \sum(\textbf{scoreCt})\right)^{val}$, proportional to the count ct of that score among the instances.

This formulation reflects our **design principles**: all instances with the same score have equivalent resilience impact and are interchangeable; instances with higher scores dominate the resilience contribution of the group; the penalty introduced by a less resilient instance decreases exponentially with increasing val, ensuring that multiple moderately good instances never outweigh the impact of one high-quality instance; and with the diminishing factor ΔD set to 1, consistent with the granularity of the five-point scale, the aggregated score is guaranteed to never drop below the next lower meaningful score.

This best-score-dominant aggregation strategy applies to all attributes whose resilience behavior follows this pattern, including $f_{pa1,inst}$, $f_{pa1,serv}$, $f_{pa2,inst}$, $f_{pa2,serv}$, $f_{cp1,inst}$, $f_{ca1,inst}$, $f_{ca1,serv}$, $f_{ca2,serv}$, $f_{ca3,serv}$ and $f_{ca4,serv}$, as indicated in Fig. 6.

4.3.2 Aggregating scores dominated by the worst case. Five attributes, including `PP1-2`, `CP2`, `DP1`, and `DA1`, exhibit propagational behavior in which overall resilience at the upper level is predominantly determined by the worst operational practice. These attributes require an aggregation strategy opposite to the best-case-dominant logic described in §4.3.1. The corresponding algorithmic procedure is implemented in the second block of Algorithm 1 (lines #14–22).

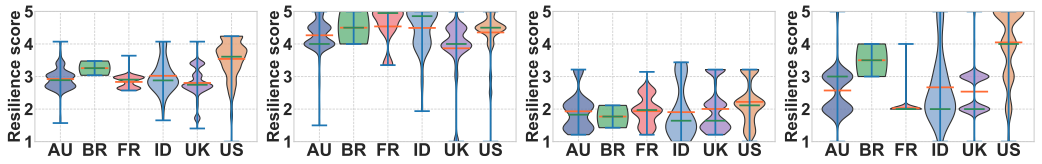
Consider `PP1`, which characterizes the hosting-enterprise type of a primary name-server instance. Because every primary instance has authority over the source zone file of a domain, an instance operated by an untrustworthy organization can propagate compromised records to all authoritative servers, potentially without detection by the domain owner. Therefore, the resilience of the primary name server is fundamentally limited by its least secure instance.

A similar pattern arises for `CP2`, which indicates whether a primary instance is co-hosted with authoritative functionality. If any instance is co-located and therefore exposed to the public Internet, the entire primary server (*e.g.,* `ns1.domain.gov`) becomes an attractive target for availability and integrity attacks [22, 23]. In such cases, the weakest configuration determines the resilience of the functionality.

Motivated by these considerations, we define a worst-score-dominant aggregation strategy. Instead of reducing a high score based on lower scores (as in the best-score-dominant strategy), this strategy begins with the worst score in the set ($s_{a,h+1,n,base}$ in line #19) and incrementally increases it by up to one score step (ΔD), depending on the count ct and values val of the better scoring instances. The denominator term $\sum(\textbf{scoreCt})^{(6-val)}$ ensures that higher-scoring instances with value val contribute larger increments, *e.g.,* a score of 5 provides the maximum uplift, while lower scores contribute exponentially diminishing increments. This prevents a few slightly better instances from overshadowing the dominance of the worst configuration. This worst-score-dominant logic is applied to attributes $f_{pp1,inst}$, $f_{pp2,inst}$, $f_{cp2,inst}$, $f_{dp1,inst}$, $f_{da1,inst}$, and $f_{da1,serv}$, as indicated in Fig. 6. As shown in our quantitative evaluation (Appendix D), both the best-case–dominant and worst-case–dominant strategies in Algorithm 1 exhibit the intended aggregation behavior.

5 Assessment Results for Government Domain Names in the Six Studied Countries

In this section, we present the assessment results and key insights obtained by applying our systematic methodology (developed in §4) to the dataset of government domains structured using our multi-sourced data schema (§3). Our analysis covers six representative countries: Australia, Brazil, France, Indonesia, the U.K., and the U.S. We begin with a comparative overview of authoritative DNS resilience across countries (§5.1), and then examine the assessment scores of all 18 infrastructure-level attributes for individual domain names. This detailed analysis highlights



(a) Overall (b) Infra. placement (c) Serv. configuration (d) Record dispatch

Fig. 8. Authoritative DNS resilience scores for government domain names in the six studied countries across: (a) overall operation, (b) infrastructure placement, (c) service configuration, and (d) record dispatch. The average values are represented as red horizontal lines.

strengths and weaknesses across the three operational phases: infrastructure placement (§5.2), service configuration (§5.3), and DNS record dispatch (§5.4).

5.1 Overview of Government Authoritative DNS Resilience in the Six Countries

Before examining the 18 attribute scores aggregated at the infrastructure level for each domain, we first provide an executive-level overview of the operational resilience (across infrastructure placement, service configuration, DNS record dispatch, and overall dimensions), summarized using the averaging functions shown in the right region of Fig. 6. The distribution of the overall resilience scores per domain name in each country is visualized in Fig. 8a, while Fig. 8 presents the distributions for each operational phase, namely placement, configuration, and dispatch.

Across all countries, the U.S. demonstrates the strongest overall operational resilience. With 1,308 unique government domain names, the second largest among the six countries, the U.S. achieves an average score of 3.5/5 and a median of 3.6/5, driven by consistently higher resilience across all three operational phases compared to the others.

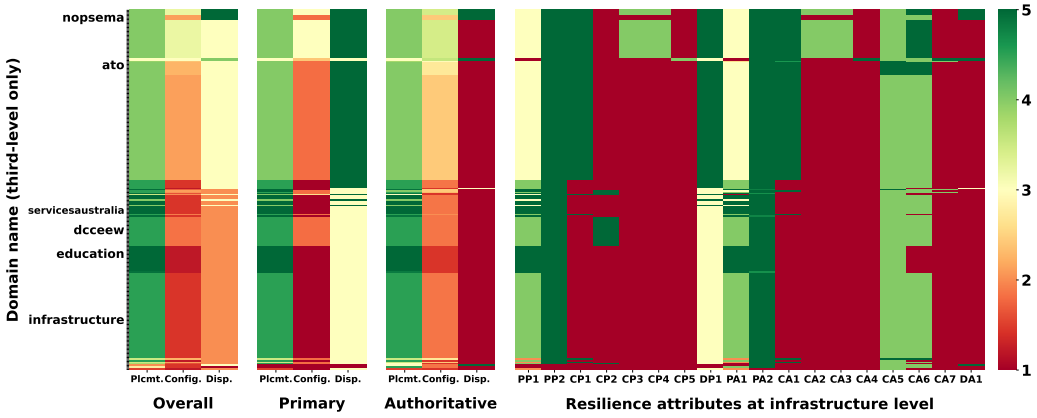
The U.K., which manages the largest number of unique government domains (5,475), exhibits mean and median scores of approximately 2.8/5, placing it near the cross-country average. Its distribution forms three distinct clusters, approximately 3.5/5 (strong), 3/5 (moderate), and 1.5/5 (weak). Although we cannot confirm administrative factors without access to confidential data, these clusters can reflect differing operational models for management practices across government agencies in the respective countries.

Australia, France, and Indonesia show relatively balanced distributions, with their average and median scores near 3/5 and without strongly separated clusters. However, France displays a small subset of domains with notably weaker resilience (below 2.9/5). Brazil, despite having only two unique government domains, each supported by a single authoritative DNS infrastructure, achieves the second-highest overall resilience, with both domains scoring 3.3/5 on average and at the median.

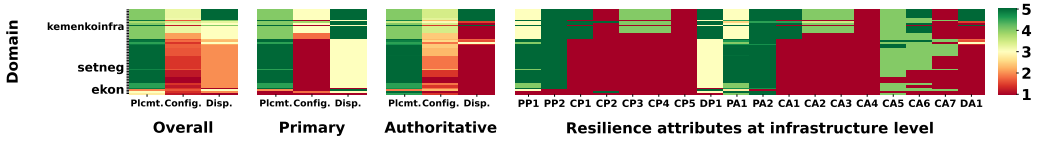
We next analyze the attribute-level assessment results at the authoritative DNS infrastructure level, highlighting the distinct strengths and weaknesses in operational practices observed across the three phases for government domain names in each country.

5.2 Resilience Scores for Infrastructure Placement Attributes

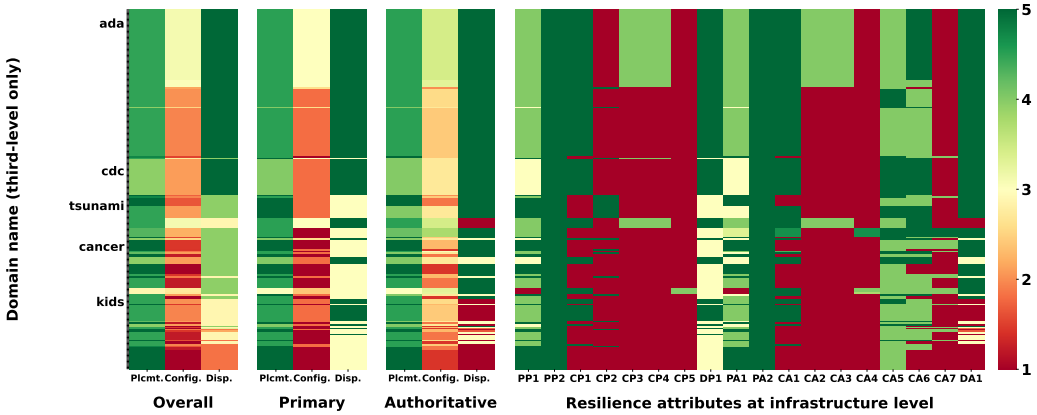
We now examine the assessment results for each government domain name, shown as rows in the heatmaps in Fig. 9 and Fig. 10. Across the `Plcmt.` column within the `Overall` blocks for each country, both **Indonesia** and **Brazil** demonstrate strong placement resilience, with nearly all domains scoring above 4/5 and almost no domains exhibiting amber or red cells (indicating scores below 3/5). This pattern is consistent across both primary and authoritative placement attributes (*i.e.,*



(a) 273 unique government domain names in **Australia**.



(b) 54 unique government domain names in **Indonesia**.



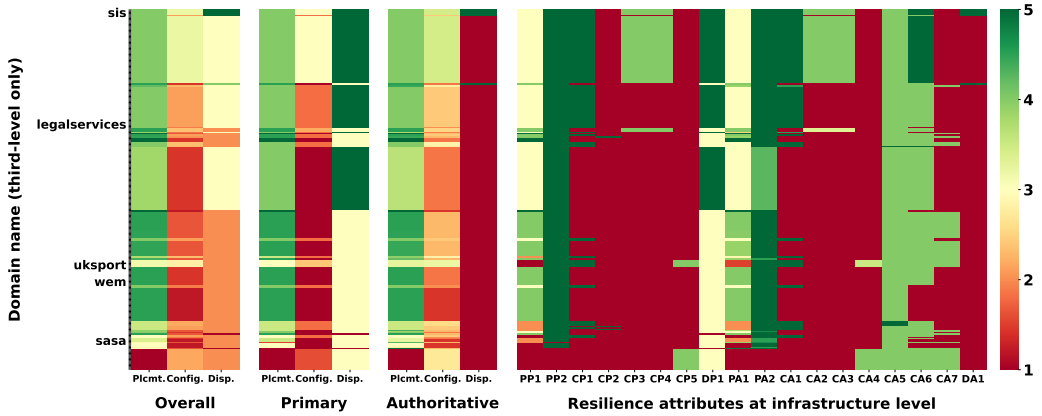
(c) 300 representative government domain names in the **U.S.**

Fig. 9. Resilience heatmaps for authoritative DNS infrastructures supporting government domains in (a) Australia, (b) Indonesia, and (c) the U.S. Each row corresponds to a domain name, and each column summarizes resilience scores across infrastructure placement, service configuration, and DNS record dispatch attributes.

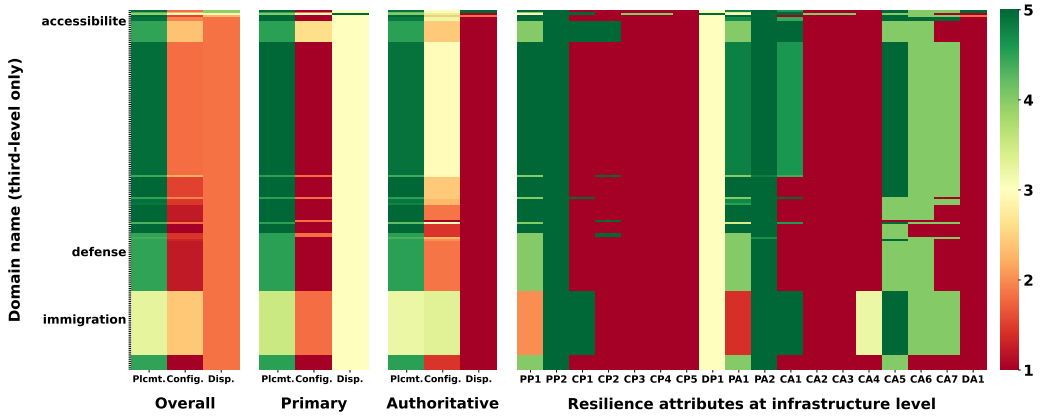
`PP1-2` and `PA1-2`), with only a few exceptions. These results likely reflect the relatively small number of government domains in both countries and their correspondingly centralized management.

For example, Brazil manages only two unique government domains `www.gov.br` and `bcb.gov.br`. All primary and authoritative name-server instances for `www.gov.br` are hosted by a Brazilian state-owned enterprise, and all instances for `bcb.gov.br` are hosted by a major cloud provider. In Indonesia, a national regulation [65] requires government digital services to be operated by the national data center (*i.e.,* SOE), and most domains comply with this requirement. The one exception is `ekon.go.id`, which delegates its primary name server to a small foreign company (as shown

(a) 2 unique government domain names in **Brazil**.



(b) 300 representative government domain names in the **U.K.**



(c) 192 unique government domain names in **France**.

Fig. 10. Resilience heatmaps for authoritative DNS infrastructures supporting government domain names in Brazil, the U.K., and France. Each row represents a domain name, and each column reflects resilience scores across placement, configuration, and dispatch attributes.

in the last row of Fig. 9b). **France** also exhibits high placement resilience for most government domains, consistent with its strict national cybersecurity regulations [7]. However, a small subset of domains perform poorly, particularly for IP administration country attributes (*i.e.,* `PP2` and `PA2`), suggesting that some servers are still hosted or administered outside national borders.

Government domains in **Australia** and the **U.K.** show more moderate placement resilience, with most domains scoring 3-4 out of 5 across the `plcmt.` columns in the `Overall`, `Primary`, and `Authoritative` blocks. This is largely driven by the attributes of the hosting provider (*i.e.,* `PP1` and `PA1`), as both countries rely extensively on US-headquartered cloud providers for authoritative DNS services. Finally, in the **U.S.**, most government domains are supported by cloud DNS infrastructures

owned and operated by US entities with domestically administrated IP address space. A small number of domains rely on SOEs or private SMEs, but these exceptions do not significantly affect the overall resilience profile of placement.

Key takeaway

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.

5.3 Resilience Scores for Service Configuration Attributes

We now examine resilience scores for service-configuration practices, as reflected in the `Config.` column and the underlying attributes `CP1-5` and `CA1-7` across the six countries studied. While configurations vary widely between individual domain names, three broad patterns emerge.

Overall, service-configuration is modest in all six countries, with most domains scoring between 2 and 3 out of 5. Among them, the **U.S.** (Fig. 9c) demonstrates the strongest performance, with the `Config.` columns dominated by amber-colored cells in, indicating comparatively better configuration practices than those observed in other countries, where orange and light-red cells are more common. Weak resilience is most pronounced for the primary functionality, especially in `CP5` (AS redundancy), a challenge shared across all domains. Maintaining multiple autonomous systems for redundancy is operationally costly, making it difficult for domain operators to adopt this best practice. Even so, 294 U.S. domains (22.48% of 1,308) do exhibit strong redundancy in hosting IPs and subnets, as indicated by higher scores in `CP3-4` and `CA2-3`.

Surprisingly, co-hosting authoritative and primary name-server functionality (indicated by `CP2`) is common across all six countries. Although operationally convenient, co-hosting exposes the primary name server, a critical, non-public function, to unnecessary Internet-facing attack surfaces.

Government domains in **Australia** (Fig. 9a) and the **U.K.** (Fig. 10b) show slightly lower configuration resilience compared to the U.S. These domains frequently score poorly in regional accessibility (indicated by `CP1`) and in redundancy across IPs (by `CP3` and `CA2`) and subnets (by `CP4` and `CA3`), especially when compared to the U.S.

Interestingly, the countries with the strongest infrastructure placement resilience, **Indonesia** (Fig. 9b), **Brazil** (Fig. 10a), and **France** (Fig. 10c), often exhibit the weakest service configurations. This contrast may reflect limited operational capacity among local hosting enterprises, despite strong placement policies. Nonetheless, there are exceptions. For example, `accessibilite.gouv.fr` achieves strong configuration resilience, with Anycast-enabled regional accessibility (*i.e.,* `CP1` and `CA1`) and separation of primary and authoritative (*i.e.,* `CP2`) implemented by a French provider.

Key takeaway

All studied 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.

5.4 Resilience Scores for DNS Record Dispatch Attributes

Reflected in `Disp.`, `DP1` and `DA1` columns, government domains in the **U.S.** demonstrate the strongest resilience in record dispatch among the six countries. Most US domains display amber or green cell

(scores 3-5) for both primary and authoritative functions. A substantial majority, 1,042 domains (79.66%), deploy DNSSEC on authoritative servers to protect DNS responses against hijacking or manipulations, with 953 domains (72.86%) using algorithms recommended by RFC8624 [78].

For primary servers, almost all government domains across all countries, except for isolated cases such as `fha.gov`, have AXFR (*i.e.,* `DP1`) enforced either manually or automatically. Instances with a red `DP1` score (no AXFR enforcement), although rare, pose meaningful risks by permitting unauthorized retrieval of authoritative DNS records.

Government domains in **Australia**, **Indonesia**, the **U.K.**, and **Brazil** exhibit weaker resilience in the record dispatch phase, primarily due to the absence of DNSSEC on their authoritative name servers (*i.e.,* `DA1`). Without DNSSEC, authoritative responses remain vulnerable to on-path manipulation even when AXFR is correctly enforced at the primary server.

Among the six countries, **France** displays the most concerning resilience profile for DNS record dispatch. Except for `dmp.gouv.fr`, all French government domains rely on manual enforcement of AXFR for primary servers, introducing additional operational risk through human-dependent configuration. Only three domains (including `finances.gouv.fr`, `culture.gouv.fr`, and `douanne.gouv.fr`) implement DNSSEC, though all three correctly use recommended algorithms. The near absence of DNSSEC deployment reduces resilience against data-integrity attacks.

Key takeaway

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.

6 Related Work

Assessing resilience of government public services: Given the criticality of public services for both taxpayers and governments, evaluating the resilience of digital infrastructures that support these services has been an active topic in the measurement community. Prior works typically study isolated components of the ecosystem. Kumar *et al.* [42] analyze the resilience from the perspective of website-hosting infrastructures for government services worldwide, focusing on the organizational profile of hosting entities (*e.g.,* third-party providers vs. domestic providers). Habib *et al.* [28] quantify the dependence of web infrastructures, including those supporting government portals, on geopolitical factors in 150 countries. Houser *et al.* [32] evaluate the availability and legitimacy of DNS records served by authoritative name servers for public-service domains. Sommese *et al.* [74] assess redundancy in recursive DNS resolution paths for government domains in the U.S., Netherlands, Sweden, and Switzerland. Jonker *et al.* [37] study longitudinal changes in Russia's digital-infrastructure ecosystem, including naming, hosting, and certificate issuance, under resilience and sovereignty pressures. To the best of our knowledge, our work is the first to evaluate the resilience of authoritative DNS infrastructures with a holistic view of the network operational process, spanning infrastructure placement, service configuration, and record dispatch.

Analyzing resilience and security of DNS infrastructure: Beyond government-specific studies, a substantial body of literature examines the resilience and security of DNS infrastructure more broadly. The work in [81] provides a large-scale characterization of DNS behavior, query failures, and underlying causes, including those relevant to DNS infrastructure. Several works identify integrity risks and configuration vulnerabilities in resolver infrastructures [15, 31, 46, 53, 66, 80, 82]. Cross-country dependency analyses [39, 41] evaluate geopolitical intergovernmental factors that shape DNS operational resilience. Another line of research studies confidentiality attacks, including domain hijacking, that exploit weaknesses in DNS service operation [5, 6, 17, 59, 73, 83].

Complementary efforts [10, 24, 34, 35, 40, 48, 52, 57, 84] examine DNS end-host behavior, including deployment of encrypted DNS protocols [18, 61, 67, 72], enterprise DNS-query patterns [50, 51], and DNS-based attacks such as reflection, resource exhaustion, and query amplification [19, 45, 58, 60]. These works highlight the security and performance implications of resolver design, encryption, and attacker behavior. Complementing prior studies, our work is the first to systematically assess the **authoritative** DNS infrastructure of a domain through the lens of its full network operational process. By modeling placement decisions, configuration practices, and record-dispatch mechanisms, we surface resilience issues that are inherently distributed and often overlooked by domain owners.

7 Discussion on Limitations

We acknowledge the limitations identified in our proposed methodology. To assign assessment scores for each attribute, we adopt a five-point Likert scale that serves as a diagnostic heuristic. The score aggregation from server instances to the overall infrastructure level uses impact-driven strategies that reflect our heuristic design principles from best practices and expert judgment. Additionally, evaluating our assessment method against real-world outages caused by resilience-related practices is beyond the scope of this work. Therefore, further investigations such as systematic sensitivity analysis and empirical validation against real-world outcomes are valuable future works. For example, assessment scores of each domain can be correlated with observed real-world outages caused by various factors described by the resilience attributes. A more systematic sensitivity analysis over score aggregation weight (beyond the analysis in Appendix E) can help clarify the intended use of our assessment framework and reduce the risk of over-interpreting the quantitative scores. Also, additional signals such as routing security can be further incorporated in our assessment framework to provide a more comprehensive coverage of resilience aspects.

8 Conclusion

We presented a systematic framework to assess the network operational resilience of authoritative DNS infrastructures supporting public-service domains operated by government agencies. Designed to serve both strategic policymakers (who require an aggregated understanding of national DNS resilience) and the individual departments responsible for operating these infrastructures, our scoring-based methodology evaluates a comprehensive set of attributes derived from a multi-sourced data schema. These attributes capture operational practices at four hierarchical levels of the authoritative DNS infrastructure and across three phases of the network operational process. We applied our framework to government domain names published by six representative countries and analyzed the resulting dataset. The assessment 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 systematic resilience, and for domain owners to identify weaknesses and improve operational practices in their DNS configurations.

Acknowledgment

We thank our anonymous shepherd and the anonymous reviewers for their insightful feedback and suggestions that helped us further improve the clarity and quality of this paper.

References

[1] ACSC. 2025. Annual Cyber Threat Report 2024-2025. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025 Accessed: 2025-11-11.

[2] AGOR. 2025. AGOR Quarterly Report. https://www.finance.gov.au/government/managing-commonwealth-resources/structure-australian-government-public-sector Accessed: 2025-07-21.

[3] Akamai. 2025. Designing DNS for Availability and Resilience Against DDoS Attacks. https://www.akamai.com/resources/white-paper/designing-dns-for-availability-and-resilience-against-ddos-attacks Accessed: 2025-11-28.
[4] Akamai. 2025. Edge DNS. https://www.akamai.com/products/edge-dns Accessed: 2025-12-01.
[5] Gautam Akiwate, Raffaele Sommese, Mattijs Jonker, Zakir Durumeric, KC Claffy, Geoffrey M. Voelker, and Stefan Savage. 2022. Retroactive identification of targeted DNS infrastructure hijacking. In *Proc. ACM IMC*. Nice, France.
[6] Eihal Alowaisheq, Siyuan Tang, Zhihao Wang, Fatemah Alharbi, Xiaojing Liao, and XiaoFeng Wang. 2020. Zombie Awakening: Stealthy Hijacking of Active Domains through DNS Hosting Referral. In *Proc. ACM CCS*. Virtual Event.
[7] ANSSI. 2025. French Cybersecurity Agency. https://cyber.gouv.fr/ Accessed: 2025-11-14.
[8] Mahdi Arghavani, Haibo Zhang, David Eyers, and Abbas Arghavani. 2024. SUSS: Improving TCP Performance by Speeding Up Slow-Start. In *Proc. ACM SIGCOMM*. Sydney, NSW, Australia.
[9] Brazil Government. 2025. Órgãos do Governo. https://www.gov.br/pt-br/orgaos-do-governo/ministerios-e-orgaos-com-status-de-ministerios Accessed: 2025-11-03.
[10] Rishabh Chhabra, Paul Murley, Deepak Kumar, Michael Bailey, and Gang Wang. 2021. Measuring DNS-over-HTTPS performance around the world. In *Proc. ACM IMC*. Virtual Event.
[11] Cloudflare. 2020. Improving DNS security, performance, and reliability. https://www.cloudflare.com/en-au/improving-dns-security-performance-reliability/ Accessed: 2025-11-28.
[12] Cloudflare. 2025. Cloudflare DNS. https://www.cloudflare.com/application-services/products/dns/ Accessed: 2025-12-01.
[13] CSIS. 2025. Significant Cyber Incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents Accessed: 2025-11-11.
[14] Cybersecurity and Infrastructure Security Agency. 2025. get.gov. https://get.gov/about/data/ Accessed: 2025-04-20.
[15] Rasmus Dahlberg and Tobias Pulls. 2023. Timeless Timing Attacks and Preload Defenses in Tor's DNS Cache. In *Proc. USENIX Security*. Anaheim, CA, USA.
[16] datagouv. 2022. Lists of gouv.fr sites. https://www.data.gouv.fr/datasets/listes-des-sites-gouv-fr/ Accessed: 2022-07-22.
[17] Casey Deccio, Alden Hilton, Michael Briggs, Trevin Avery, and Robert Richardson. 2020. Behind Closed Doors: A Network Tale of Spoofing, Intrusion, and False DNS Security. In *Proc. ACM IMC*. Virtual Event, USA.
[18] Hongying Dong, Yizhe Zhang, Hyeonmin Lee, Shumon Huque, and Yixin Sun. 2024. Exploring the Ecosystem of DNS HTTPS Resource Records: An End-to-End Perspective. In *Proc. ACM IMC*. Madrid, Spain.
[19] Huayi Duan, Marco Bearzi, Jodok Vieli, David Basin, Adrian Perrig, Si Liu, and Bernhard Tellenbach. 2024. CAMP: Compositional Amplification Attacks against DNS. In *Proc. USENIX Security*. Philadelphia, PA, USA.
[20] Ludwig Englbrecht, Stefan Meier, and Günther Pernul. 2020. Towards a Capability Maturity Model for Digital Forensic Readiness. *Wireless Networks* 26, 7 (Oct. 2020).
[21] European Commision. 2025. Digital Tracking. https://commission.europa.eu/strategy-and-policy/eu-budget/performance-and-reporting/horizontal-priorities/digital-tracking_en Accessed: 2025-11-11.
[22] Evans, Julia. 2022. Why might you run your own DNS server? https://jvns.ca/blog/2022/01/05/why-might-you-run-your-own-dns-server-/ Accessed: 2025-11-28.
[23] ExamLabs. 2025. Understanding the Role of DNS Authoritative Name Servers. https://www.exam-labs.com/blog/understanding-the-role-of-dns-authoritative-name-servers Accessed: 2025-11-28.
[24] Tillson Galloway, Kleanthis Karakolios, Zane Ma, Roberto Perdisci, Angelos Keromytis, and Manos Antonakakis. 2024. Practical Attacks Against DNS Reputation Systems. In *Proc. IEEE S&P*.
[25] Google. 2025. Cloud DNS. https://cloud.google.com/dns/ Accessed: 2025-12-01.
[26] Government Digital Service and Central Digital and Data Office. 2025. List of .gov.uk domain names. https://www.gov.uk/government/publications/list-of-gov-uk-domain-names Accessed: 2025-07-22.
[27] Harm Griffioen, Georgios Koursiounis, Georgios Smaragdakis, and Christian Doerr. 2024. Have you SYN me? Characterizing Ten Years of Internet Scanning. In *Proc. ACM IMC*. Madrid, Spain.
[28] Rumaisa Habib, Kimberly Ruth, Gautam Akiwate, and Zakir Durumeric. 2025. Formalizing Dependence of Web Infrastructure. In *Proc. ACM SIGCOMM*. São Francisco Convent, Coimbra, Portugal.
[29] Elias Heftrig, Haya Schulmann, Niklas Vogel, and Michael Waidner. 2024. The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC. In *Proc. ACM CCS*.
[30] Raphael Hiesgen, Marcin Nawrocki, Marinho Barcellos, Daniel Kopp, Oliver Hohlfeld, Echo Chan, Roland Dobbins, Christian Doerr, Christian Rossow, Daniel R. Thomas, Mattijs Jonker, Ricky Mok, Xiapu Luo, John Kristoff, Thomas C. Schmidt, Matthias Wählisch, and kc claffy. 2024. The Age of DDoScovery: An Empirical Comparison of Industry and Academic DDoS Assessments. In *Proc. ACM IMC*. Madrid, Spain.
[31] Alden Hilton, Casey Deccio, and Jacob Davis. 2023. Fourteen Years in the Life: A Root Server's Perspective on DNS Resolver Security. In *Proc. USENIX Security*. Anaheim, CA, USA.
[32] Rebekah Houser, Shuai Hao, Chase Cotton, and Haining Wang. 2022. A Comprehensive, Longitudinal Study of Government DNS Deployment at Global Scale. In *Proc. IEEE/IFIP DSN*.

[33] IPinfo. 2025. IPinfo: The Trusted Source For IP Address Data. https://ipinfo.io Accessed: 2025-11-14.
[34] Katsuki Isobe, Daishi Kondo, and Hideki Tode. 2022. A first look at the name resolution latency on handshake. In *Proc. ACM IMC*. Nice, France.
[35] Liz Izhikevich, Gautam Akiwate, Briana Berger, Spencer Drakontaidis, Anna Ascheman, Paul Pearce, David Adrian, and Zakir Durumeric. 2022. ZDNS: a fast DNS toolkit for internet measurement. In *Proc. ACM IMC*. Nice, France.
[36] Akshath Jain, Deepayan Patra, Peijing Xu, Justine Sherry, and Phillipa Gill. 2022. The ukrainian internet under attack: an NDT perspective. In *Proc. ACM IMC*. Nice, France.
[37] Mattijs Jonker, Gautam Akiwate, Antonia Affinito, kc Claffy, Alessio Botta, Geoffrey M. Voelker, Roland van Rijswijk-Deij, and Stefan Savage. 2022. Where .ru? Assessing the Impact of Conflict on Russian Domain Infrastructure. In *Proc. ACM IMC*. Nice, France.
[38] Joshi, Sagar. 2025. 10 Biggest IT Outages in History: Who Pulled the Plug? https://learn.g2.com/biggest-it-outages-in-history Accessed: 2025-12-01.
[39] Aqsa Kashaf, Vyas Sekar, and Yuvraj Agarwal. 2020. Analyzing Third Party Service Dependencies in Modern Web Services: Have We Learned from the Mirai-Dyn Incident?. In *Proc. ACM IMC*. Virtual Event.
[40] Mike Kosek, Luca Schumann, Robin Marx, Trinh Viet Doan, and Vaibhav Bajpai. 2022. DNS privacy with speed? evaluating DNS over QUIC and its impact on web performance. In *Proc. ACM IMC*. Nice, France.
[41] 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).
[42] Rashna Kumar, Esteban Carisimo, Lukas De Angelis Riva, Mauricio Buzzone, Fabián E. Bustamante, Ihsan Ayyub Qazi, and Mariano G. Beiró. 2024. Of Choices and Control - A Comparative Analysis of Government Hosting. In *Proc. ACM IMC*. Madrid, Spain.
[43] Jungjae Lee, Yubin Choi, Minhyuk Song, and Sanghyun Park. 2024. ChatFive: Enhancing User Experience in Likert Scale Personality Test through Interactive Conversation with LLM Agents. In *Proc. ACM CUI*. Luxembourg, Luxembourg.
[44] Edward P. Lewis and Alfred Hoenes. 2010. DNS Zone Transfer Protocol (AXFR). RFC 5936.
[45] Xiang Li, Dashuai Wu, Haixin Duan, and Qi Li. 2024. DNSBomb: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses. In *IEEE Symposium on Security and Privacy*.
[46] 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*.
[47] Kurt Erik Lindqvist and Joe Abley. 2006. Operation of Anycast Services. RFC 4786.
[48] Guannan Liu, Lin Jin, Shuai Hao, Yubao Zhang, Daiping Liu, Angelos Stavrou, and Haining Wang. 2023. Dial "N" for NXDomain: The Scale, Origin, and Security Implications of DNS Queries to Non-Existent Domains. In *Proc. ACM IMC*. Montreal QC, Canada.
[49] Minzhao Lyu. 2026. Critical Infrastructure Measurement Dataset. https://minzhaolyu.github.io/dataset/InternetInfrastructureDataset Accessed: 2026-03-19.
[50] Minzhao Lyu, Hassan Habibi Gharakheili, Craig Russell, and Vijay Sivaraman. 2021. Hierarchical Anomaly-Based Detection of Distributed DNS Attacks on Enterprise Networks. *IEEE TNSM* 18, 1 (2021).
[51] Minzhao Lyu, Hassan Habibi Gharakheili, Craig Russell, and Vijay Sivaraman. 2023. Enterprise DNS Asset Mapping and Cyber-Health Tracking via Passive Traffic Analysis. *IEEE TNSM* 20, 3 (2023).
[52] Minzhao Lyu, Hassan Habibi Gharakheili, and Vijay Sivaraman. 2022. Classifying and tracking enterprise assets via dual-grained network behavioral analysis. *Computer Networks* 218 (2022).
[53] Keyu Man, Xin'an Zhou, and Zhiyun Qian. 2021. DNS Cache Poisoning Attack: Resurrections with Side Channels. In *Proc. ACM CCS*. Virtual Event.
[54] McLeod, Saul. 2025. Likert Scale Questionnaire: Examples & Analysis. https://www.simplypsychology.org/likert-scale.html Accessed: 2025-12-01.
[55] Mitchell, Robert. 2025. What Is Internet Resilience? https://www.internetsociety.org/blog/2025/08/what-is-internet-resilience/ Accessed: 2025-11-11.
[56] Moss, Sebastian. 2025. 8.8 magnitude earthquake causes Internet outages in Kamchatka, Russia. https://www.datacenterdynamics.com/en/news/88-magnitude-earthquake-causes-internet-outages-in-kamchatka-russia/ Accessed: 2025-10-30.
[57] Giovane C. M. Moura, Sebastian Castro, Wes Hardaker, Maarten Wullink, and Cristian Hesselman. 2020. Clouding up the Internet: how centralized is DNS traffic becoming?. In *Proc. ACM IMC*. Virtual Event.
[58] Giovane C. M. Moura, Sebastian Castro, John Heidemann, and Wes Hardaker. 2021. TsuNAME: exploiting misconfiguration and vulnerability to DDoS DNS. In *Proc. ACM IMC* (Virtual Event).
[59] Giovane C. M. Moura, Thomas Daniels, Maarten Bosteels, Sebastian Castro, Moritz Müller, Thymen Wabeke, Thijs van den Hout, Maciej Korczyński, and Georgios Smaragdakis. 2024. Characterizing and Mitigating Phishing Attacks at ccTLD Scale. In *Proc. ACM CCS*.

[60] Marcin Nawrocki, Mattijs Jonker, Thomas C. Schmidt, and Matthias Wählisch. 2021. The far side of DNS amplification: tracing the DDoS attack ecosystem from the internet core. In *Proc. ACM IMC* (Virtual Event).
[61] Alexandra Nisenoff, Ranya Sharma, and Nick Feamster. 2023. User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers. In *Proc. USENIX Security*. Anaheim, CA, USA.
[62] Fariba Osali, Khwaja Zubair Sediqi, and Oliver Gasser. 2025. Sibling Prefixes: Identifying Similarities in IPv4 and IPv6 Prefixes. In *Proc. ACM IMC*. USA.
[63] Pallarito, Ash and Abley, Joe. 2022. Cloudflare 1.1.1.1 incident on July 14, 2025. https://blog.cloudflare.com/cloudflare-1-1-1-1-incident-on-july-14-2025/ Accessed: 2025-11-11.
[64] Michael A. Patton, Scott O. Bradner, Robert Elz, and Randy Bush. 1997. Selection and Operation of Secondary DNS Servers. RFC 2182.
[65] Presiden Republik Indonesia. 2018. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018 Accessed: 2025-11-12.
[66] Audrey Randall, Enze Liu, Gautam Akiwate, Ramakrishna Padmanabhan, Geoffrey M. Voelker, Stefan Savage, and Aaron Schulman. 2020. Trufflehunter: Cache Snooping Rare Domains at Large Public DNS Resolvers. In *Proc. ACM IMC* (Virtual Event).
[67] Audrey Randall, Enze Liu, Ramakrishna Padmanabhan, Gautam Akiwate, Geoffrey M. Voelker, Stefan Savage, and Aaron Schulman. 2021. Home is where the hijacking is: understanding DNS interception by residential routers. In *Proc. ACM IMC*. Virtual Event.
[68] RDAP.org. 2025. The Registration Data Access Protocol. https://about.rdap.org Accessed: 2025-11-01.
[69] Robinson, Dan. 2025. A single DNS race condition brought Amazon's cloud empire to its knees. https://www.theregister.com/2025/10/23/amazon_outage_postmortem/ Accessed: 2025-11-11.
[70] Secretary of State Science. 2025. State of digital government review. https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review Accessed: 2025-08-11.
[71] Sekretaris Kabinet Republik Indonesia. 2024. Kabinet Pemerintahan Indonesia. https://setkab.go.id/profil-kabinet/ Accessed: 2025-11-12.
[72] Raffaele Sommese, Gautam Akiwate, Antonia Affinito, Moritz Muller, Mattijs Jonker, and kc claffy. 2024. DarkDNS: Revisiting the Value of Rapid Zone Update. In *Proc. ACM on IMC*. Madrid, Spain.
[73] Raffaele Sommese, KC Claffy, Roland van Rijswijk-Deij, Arnab Chattopadhyay, Alberto Dainotti, Anna Sperotto, and Mattijs Jonker. 2022. Investigating the impact of DDoS attacks on DNS infrastructure. In *Proc. ACM IMC*. Nice, France.
[74] Raffaele Sommese, Mattijs Jonker, Jeroen van der Ham, and Giovane C. M. Moura. 2022. Assessing e-Government DNS Resilience. In *Proc. International Conference on Network and Service Management*.
[75] Florian Steurer, Amreesh Phokeer, Philip Paeps, and Liz Izhikevich. 2025. Measuring Resilience of Authoritative DNS. In *Proc. ACM SIGCOMM Posters and Demos*. Coimbra, Portugal.
[76] United Nation. 2024. E-Government Development Index (EGDI). https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index Accessed: 2025-08-22.
[77] U.S. Congress. 2024. Information Technology Spending in the President's Budget Submission for FY2025: In Brief. https://www.congress.gov/crs-product/R48049 Accessed: 2025-11-11.
[78] Paul Wouters and Ondřej Surý. 2019. Algorithm Implementation Requirements and Usage Guidance for DNSSEC. RFC 8624. https://www.rfc-editor.org/info/rfc8624
[79] Yunpeng Xing, Chaoyi Lu, Baojun Liu, Haixin Duan, Junzhe Sun, and Zhou Li. 2024. Yesterday Once More: Global Measurement of Internet Traffic Shadowing Behaviors. In *Proc. ACM IMC*. Madrid, Spain.
[80] Wei Xu, Xiang Li, Chaoyi Lu, Baojun Liu, Haixin Duan, Jia Zhang, Jianjun Chen, and Tao Wan. 2023. TsuKing: Coordinating DNS Resolvers and Queries into Potent DoS Amplifiers. In *Proc. ACM CCS*. Copenhagen, Denmark.
[81] 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.
[82] Yehuda Afek and Anat Bremler-Barr and Shani Stajnrod. 2023. NRDelegationAttack: Complexity DDoS attack on DNS Recursive Resolvers. In *Proc. USENIX Security*. Anaheim, CA, USA.
[83] Fenglu Zhang, Baojun Liu, Eihal Alowaisheq, Jianjun Chen, Chaoyi Lu, Linjian Song, Yong Ma, Ying Liu, Haixin Duan, and Min Yang. 2023. Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers. In *Proc. ACM CCS*. Copenhagen, Denmark.
[84] Yunyi Zhang, Baojun Liu, Haixin Duan, Min Zhang, Xiang Li, Fan Shi, Chengxi Xu, and Eihal Alowaisheq. 2024. Rethinking the Security Threats of Stale DNS Glue Records. In *Proc. USENIX Security*. Philadelphia, PA, USA.
[85] Minyuan Zhou, Xiao Zhang, Shuai Hao, Xiaowei Yang, Jiaqi Zheng, Guihai Chen, and Wanchun Dou. 2023. Regional IP Anycast: Deployments, Performance, and Potentials. In *Proc. ACM SIGCOMM*. New York, NY, USA.

A Source Code and Data Availability

We make publicly available the source code of our data collection and assessment pipeline, along with the datasets collected and generated in this study. These include the authoritative DNS resilience dataset for government domains in the six studied countries (§3.2), local configurations and catalogs used in the assessment process, and the full set of assessment scores reported in §4. All resources are accessible via a permanent public link [49] on our academic website under the "Authoritative DNS Infrastructure" category.

B Data Collection and Resilience Assessment Pipeline

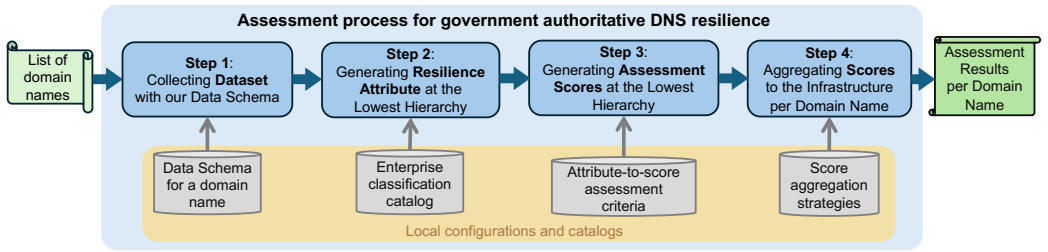


Fig. 11. Overview of our data collection and assessment pipeline for evaluating the operational resilience of authoritative DNS infrastructures supporting government services.

As shown in Fig. 11, our automated assessment pipeline comprises four stages: data collection using our data schema, generation of resilience attributes, assignment of scores on a five-point scale, and aggregation of scores to produce domain-level assessments. The pipeline accepts a CSV file listing domain names to evaluate and processes each domain name individually.

In the **first** step, the pipeline validates the existence of each domain name via DNS lookups using the Linux `dig` tool. A hierarchical JSON object is then instantiated to store all data fields defined in our schema (Fig. 2). For each authoritative name server identified in the NS record, we query relevant DNS records: `SOA`, `NS`, `A`, `AAAA`, `DNSSEC`, and `AXFR`, from our measurement vantage points. By design, authoritative DNS records are retrieved from authoritative name servers as the only source of truth, and variation of measurement vantage points has negligible impact under normal circumstances in the absence of data integrity attacks (*e.g.,* hijacking). As an additional validation, we collect data from two vantage points: one with a public IP address in our lab and one located in the studied countries via VPN services. We also configure the DNS resolution using three options: the local ISP resolver and public resolvers operated by Google and Cloudflare. No inconsistencies are observed across these collection settings. To obtain registration information, the pipeline uses the Python IPWhois API to retrieve RDAP records (`rdap.org`) for every IP address associated with primary and authoritative name-server instances. The IP operational attributes (*e.g.,* Anycast status) are collected using the IPInfo Python API. Similarly, no inconsistency are observed from across vantage points, as both RDAP and IPInfo rely on centrally maintained databases.

In the **second** step, all collected fields are converted into the 18 resilience attributes defined in §4.1. This includes mapping hosting-enterprise names to their corresponding categories using a curated enterprise-classification catalog (stored in JSON), converting geolocations to country codes, enumerating string-valued fields, counting server instances and name servers, and identifying unique administrative subnets and ASes. In the **third** step, each attribute is evaluated according to its scoring criteria in Table 2. These criteria are implemented as modular scoring functions configured through a YAML file, allowing assessors to modify the scoring logic without altering

Table 2. Resilience attributes at their finest hierarchical levels, together with the criteria and five-point scores used in our assessment.

NS Function	Assessment aspect	Attribute	Hierarchy	Assessment criteria	Score
Infrastructure placement					
Primary	Hosting enterprise type	**PP1**	***Instance***	State-owned enterprise	5
				Local private enterprise	4
				Foreign large enterprise	3
				Foreign SME enterprise	2
				Unregistered enterprise	1
	Hosting geolocation	**PP2**	***Instance***	Inside the country	5
				Outside the country	1
Authoritative	Hosting enterprise type	**PA1**	***Instance***	State-owned enterprise	5
				Local private enterprise	4
				Foreign large enterprise	3
				Foreign SME enterprise	2
				Unregistered enterprise	1
	Hosting geolocation	**PA2**	***Instance***	Inside the country	5
				Outside the country	1
Service configuration					
Primary	Regional accessibility	**CP1**	***Instance***	Anycast implemented	5
				Anycast not implemented	1
	Public exposure	**CP2**	***Instance***	Instance is listed in authoritative NS	5
				IP is not listed in authoritative NS	1
	Instance redundancy	**CP3**	***Name server***	More than 4 IPs used for the name server	5
				2, 3, or 4 IPs used for the name server	4
				1 IP used for the name server	1
	Subnet redundancy - name server	**CP4**	***Name server***	More than 4 subnets used for the name server	5
				2, 3, or 4 subnets used for the name server	4
				1 subnet used for the name server	1
	AS redundancy - name server	**CP5**	***Name server***	More than 4 ASes used for the name server	5
				2, 3, or 4 ASes used for the name server	4
				1 AS used for the name server	1
Authoritative	Regional accessibility	**CA1**	***Instance***	Anycast implemented	5
				Anycast not impemented	1
	Instance redundancy	**CA2**	***Name server***	More than 4 IPs used for the name server	5
				2, 3, or 4 IPs used for the name server	4
				1 IP used for the name server	1
	Subnet redundancy - name server	**CA3**	***Name server***	More than 4 subnets used for the name server	5
				2, 3, or 4 subnets used for the name server	4
				1 subnet used for the name server	1
	AS redundancy - name server	**CA4**	***Name server***	More than 4 ASes used for the name server	5
				2, 3, or 4 ASes used for the name server	4
				1 AS used for the name server	1
	Name server redundancy	**CA5**	***NS functionality***	More than 4 authoritative name servers used	5
				2, 3, or 4 name servers used	4
				1 name server used	1
	Subnet redundancy - NS function	**CA6**	***NS functionality***	More than 4 subnets used for the NS functionality	5
				2, 3, or 4 subnets used for the NS functionality	4
				1 subnet used for the NS functionality	1
	AS redundancy - NS function	**CA7**	***NS functionality***	More than 4 ASes used for the NS functionality	5
				2, 3, or 4 ASes used for the NS functionality	4
				1 AS used for the NS functionality	1
DNS record dispatch					
Primary	Zone file delivery	**DP1**	***Instance***	Automatic AXFR enforcement	5
				Manual AXFR enforcement	3
				AXFR not enforced	1
Authoritative	DNS response delivery	**DA1**	***Instance***	Recommended DNSSEC algorithm	5
				Not recommended DNSSEC algorithm	3
				DNSSEC not implemented	1

the core pipeline. Lastly, in the **fourth** and final step, the pipeline aggregates attribute scores from their lowest hierarchical level upward, following the strategies shown in Fig. 6. Depending on the attribute, aggregation uses direct mapping, the worst-score-dominant strategy, or the best-score-dominant strategy, as specified in a YAML configuration file. The resulting JSON output contains all attributes and their scores throughout the hierarchy for the assessed domain. These aggregated results for government domains in the six studied countries are analyzed in §5.

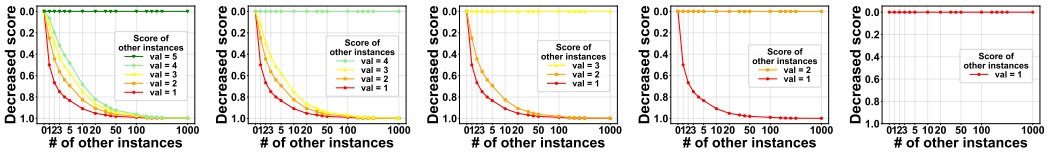
C List of Authoritative DNS Resilience Attributes and Assessment Criteria

Table 2 summarizes all resilience attributes used in our assessment of authoritative DNS infrastructures for government domains. Each attribute captures a unique aspect of operational practice,

categorized by the operational phase, DNS functionality, and assessment dimension. All attributes are defined at their finest applicable hierarchy level, as described in §4.1. The last two columns of Table 2 present the assessment criteria and corresponding five-point scores assigned to each attribute, following the scoring methodology discussed in §4.2.

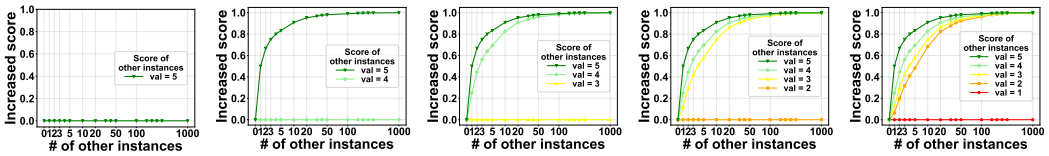
D Simulation Results of Our Score Aggregation Strategies

To evaluate whether the two score-aggregation strategies in Algorithm 1 behave as intended, as described in §4.3, we conducted simulations using extensive combinations of score arrays $\mathbf{s}_{a,h,n}$ comprising different counts of values from the set $\{1, \ldots, 5\}$. The simulations cover realistic configurations (reflecting the small numbers of instances and name servers commonly observed in our dataset) and theoretical upper bounds, with array lengths increasing up to 1000 elements to demonstrate convergence behavior.



(a) $s_{a,h+1,base} = 5$. (b) $s_{a,h+1,base} = 4$. (c) $s_{a,h+1,base} = 3$. (d) $s_{a,h+1,base} = 2$. (e) $s_{a,h+1,base} = 1$.

Fig. 12. Simulation of the **best**-score-dominant strategy in Algorithm 1, showing aggregated outcomes for $s_{a,h+1,base}$ set to: (a) 5, (b) 4, (c) 3, (d) 2, and (e) 1. Each subfigure shows boundary cases with one best-scoring instance and all remaining instances sharing the same lower score.



(a) $s_{a,h+1,base} = 5$. (b) $s_{a,h+1,base} = 4$. (c) $s_{a,h+1,base} = 3$. (d) $s_{a,h+1,base} = 2$. (e) $s_{a,h+1,base} = 1$.

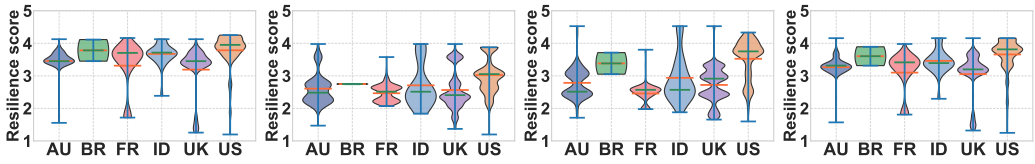
Fig. 13. Simulation of the **worst**-score-dominant strategy in Algorithm 1, showing aggregated outcomes for $s_{a,h+1,base}$ set to: (a) 5, (b) 4, (c) 3, (d) 2, and (e) 1. Each subfigure shows boundary cases with one worst-scoring instance and all remaining instances sharing the same higher score.

For the best-score-dominant aggregation strategy, Fig 12 presents the boundary cases in which the array contains exactly one score instance with the best score $\mathbf{s}_{a,h+1,base}$ while all other instances share the same lower score. As established in our design principles (§4.3), any number of instances with scores worse than the best score should never reduce the aggregated value by more than a single step $\Delta D = 1$. This property is confirmed across all five possible best values in Fig. 12a–12e, where boundary curves converge to a reduction of exactly one step. The figures also show that (i) the penalty introduced by a worse score grows exponentially as the score decreases, as seen when comparing vertical drops across values within the same plot, and (ii) the penalty is evenly distributed across, as demonstrated by horizontal shifts observed when varying the lower-scoring instances along the same curve. Aggregated scores for all other score arrays lie between the boundary curves, consistent with the expected behavior of the strategy.

For the worst-score-dominant aggregation strategy, simulation results in Fig. 13 similarly validate our design objectives. In this case, the aggregated value starts at the lowest score in the array and

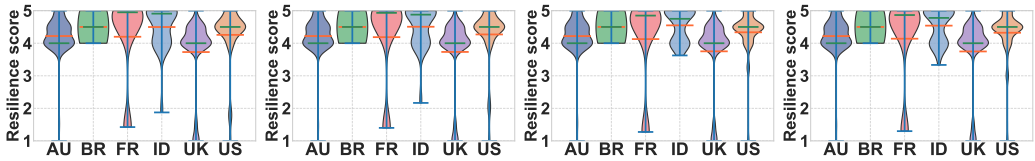
increases by at most one step $\Delta D = 1$, with increments contributed by higher-scoring instances decreasing exponentially according to Algorithm 1. The convergence trends observed in the simulated configurations confirm that the strategy precisely captures the intended dominance of the weakest configuration in determining resilience.

E Weight Sensitivity Analysis for Country-level Results



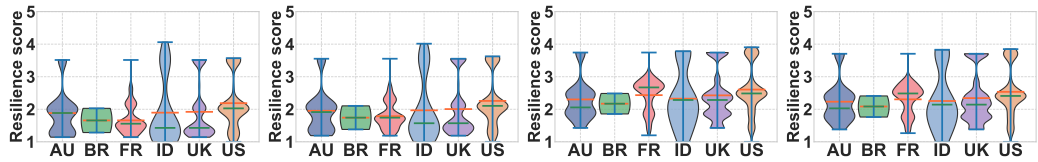
(a) Placement prioritized (b) Config. prioritized (c) Dispatch prioritized (d) Placement focused

Fig. 14. Overall authoritative DNS resilience scores for government domain names in the six studied countries with the weights of "placement", "config", and "dispatch" scores set to (a) high, low and low, (b) low, high and low (c) low, low and high, and (d) medium, low and low.



(a) Primary prioritized (b) Primary focused (c) Authori. prioritized (d) Authori. focused

Fig. 15. Authoritative DNS resilience scores in "placement" for government domain names in the six studied countries with the weights of "prim_place" and "auth_place" scores set to (a) high and low, (b) medium and low (c) low and high, and (d) low and medium.

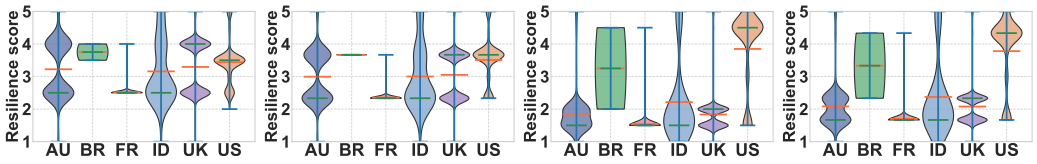


(a) Primary prioritized (b) Primary focused (c) Authori. prioritized (d) Authori. focused

Fig. 16. Authoritative DNS resilience scores in "configuration" for government domain names in the six studied countries with the weights of "prim_config" and "auth_config" scores set to (a) high and low, (b) medium and low (c) low and high, and (d) low and medium.

In §5, we present our assessment results for each country by aggregating attribute-level resilience scores to each operational phase and domain levels using equal weights. In this section, we examine how these results vary under alternative weighting schemes that emphasize different operational phases.

Fig. 14 shows the overall domain-level scores across the six countries under four weighting strategies: prioritizing placement (Fig. 14a), configuration (Fig. 14b), and dispatch (Fig. 14c) by assigning them a higher weight "3" relative to others "1", as well as a scheme that moderately



(a) Primary prioritized (b) Primary focused (c) Authori. prioritized (d) Authori. focused

Fig. 17. Authoritative DNS resilience scores in "dispatch" for government domain names in the six studied countries with the weights of "prim_disp" and "auth_disp" scores set to (a) high and low, (b) medium and low (c) low and high, and (d) low and medium.

emphasizes placement (weight "2"). Compared to the balanced results in Fig. 8a, the U.S. consistently shows the highest resilience across all schemes, while Brazil performs better when dispatch is prioritized. When configuration is emphasized, resilience scores decrease across all countries by approximately one point on the five-point scale.

We further examine the impact of weighting differences between primary and authoritative functions within each operational phase in Fig. 15, Fig. 16 and Fig. 17. The observed variations highlight the flexibility of our assessment framework, which can be adapted to different evaluation priorities and scenarios.

Received January 2026; revised March 2026; accepted April 2026