A First Look on Discovery of Designated Resolvers

Steffen Sassalla
Hasso Plattner Institute
University of Potsdam, Germany
steffen.sassalla@student.hpi.de

vasilis ververis
Hasso Plattner Institute
University of Potsdam, Germany
vasilis.ververis@hpi.de

Vaibhav Bajpai
Hasso Plattner Institute
University of Potsdam, Germany
vaibhav.bajpai@hpi.de

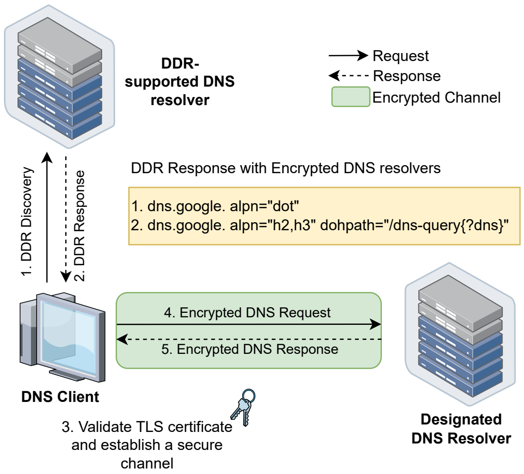
***Abstract*—DNS is crucial for the Internet but vulnerable due to plaintext traffic. Despite efforts to standardize DNS encryption, its adoption remains limited. Users often lack awareness of privacy risks and the knowledge needed to enable encryption. To address this, the IETF standardized a new protocol; Discovery of Designated Resolvers (DDR), enabling automatic discovery and upgrade from unencrypted to encrypted DNS traffic. As such, we conduct a large-scale measurement of 27 480 002 DNS resolvers in the IPv4 and IPv6 address space to evaluate DDR support. We show that 301 780 of these DNS resolvers support DDR while one in three advertised encrypted resolvers fails to reply on DNS queries. Among DDR-supported resolvers, DNS over HTTPS (DoH)/2 is the most popular advertised protocol (99.95 %), whereas DNS over QUIC (DoQ) is the least prevalent (0.84 %). Despite recent studies demonstrating the performance and privacy benefits of DoQ, this new protocol is still advertised via DDR with the lowest priority overall. Finally, 93 % of DDR resolvers share identical configurations that redirect clients to major cloud DNS providers, such as Google and Cloudflare, thereby raising critical concerns about the effectiveness of DDR deployment in addressing end-user privacy and DNS centralization.**

I. Introduction

Domain Name System (DNS) queries reveal sensitive information about the intent of a client to connect to a service on the Internet. Previous studies have shown that observing DNS queries can even allow users to be tracked across multiple websites [1], [2], [3]. Beyond tracking users online, DNS traffic can also be used to infer the presence of Internet of Things (IoT) devices at home, and may even expose information on how people use these devices [4], [5].

As awareness of end-user privacy continues to grow, significant efforts have been undertaken to secure DNS communication [6], [7], [8], [9], [10], particularly through the standardization of encrypted DNS protocols [1], commonly referred to as DNS-over-Encryption (DoE) protocols. These protocols include DNS over HTTPS (DoH) [11], DNS over TLS (DoT) [12], and the most recently standardized protocol, DNS over QUIC (DoQ) [13]. DoE protocols are principally designed to encrypt the communication between clients (e.g., stub resolvers or web browsers) and recursive resolvers through TLS, thereby securing the *stub-to-recursive* communication path.

Despite these advancements, the majority of DNS traffic remains unencrypted. For example, Cloudflare reports that 89% of DNS queries to its popular `1.1.1.1` recursive resolver remain unencrypted, with only 11% utilizing one of the aforementioned DoE protocols [14]. The manual, conventional transition from plaintext DNS to encrypted DNS poses challenges for many users [14], as it requires additional knowledge about reasoning and manual interaction. Further, none of the DoE protocols offer provisions for resolver selection by client applications to enable an automatic upgrade from plaintext to encrypted DNS. As such, clients have limited means to discover encrypted DNS resolvers and end up relying on the (often unencrypted) resolver assigned by the Internet Service Provider (ISP) via Dynamic Host Configuration Protocol (DHCP). In addition, users frequently remain unaware of the privacy risks associated with using unencrypted DNS, and there is insufficient understanding on how to effectively transition to encrypted DNS configurations. Consequently, there is a pressing need for mechanisms that enable clients to both identify available encrypted DNS services and automatically switch to them without requiring user intervention.



DDR-supported DNS resolver
Request
Response
🟩 Encrypted Channel
1. DDR Discovery
2. DDR Response
DDR Response with Encrypted DNS resolvers
1. dns.google. alpn="dot"
2. dns.google. alpn="h2,h3" dohpath="/dns-query{?dns}"
4. Encrypted DNS Request
5. Encrypted DNS Response
DNS Client
3. Validate TLS certificate and establish a secure channel
Designated DNS Resolver

Fig. 1. The DDR protocol enables discovery and automatic upgrading to encrypted DNS. An example DDR response of the designated (encrypted) DNS resolvers offered by `8.8.8.8` is shown.

To address this need, the Internet Engineering Task Force (IETF) standardized the protocol Discovery of Designated Resolvers (DDR) [15] in November 2023. DDR streamlines the adoption of encrypted DNS by enabling clients to use plaintext DNS to automatically discover DoE endpoints and their configurations, such as ports or URI paths in the case of DoH (see Figure 1). Consequently, DDR provides a mechanism for clients to seamlessly transition from plaintext DNS to encrypted DNS without requiring any user interaction.

However, to the best of our knowledge, no efforts have been made to investigate DDR. To address this critical gap, we examine the following research questions: ***a****) How many DNS resolvers support DDR over the Internet?* ***b****) What role do cloud providers (such as Google, Cloudflare, etc.) play in DDR support?* ***c****) How do resolvers that send DDR configurations prioritize different encrypted DNS protocols?* ***d****) How often do encrypted resolvers deviate from default DoE configurations like standard ports or default URI query paths (DoH)?* ***e****) What is the reliability of the discovered encrypted resolvers in responding to DNS queries?*

To address these questions, we evaluate the global DDR support

ISBN 978-3-903176-72-0 © 2025 IFIP

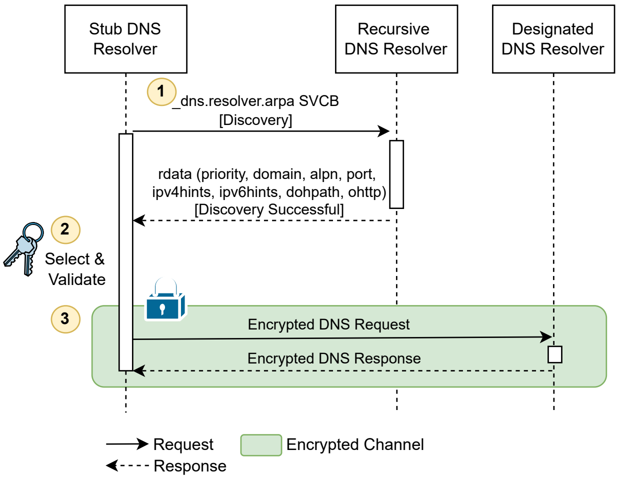


Fig. 2. Sequence diagram of DDR discovery: This diagram depicts the DDR discovery of an unencrypted resolver, designated resolver validation (e.g., certificate validation) of the designated resolver, and the encrypted communication between the stub resolver and the designated resolver through an encrypted tunnel

by querying active DNS resolvers using DDR discovery queries, as outlined in DDR's specification [15]. This methodology enables the identification of DDR-enabled DNS resolvers and of encrypted DNS resolvers including their DoE endpoints and configurations.

A. Preliminaries

When initiating a DNS request, a client typically directs the query to a recursive resolver, delegating the resolution task. These recursive resolvers, commonly managed by ISPs or other entities, may respond to the DNS query from within their cache if they already possess the desired information. In the absence of a cached response, the recursive resolver follows a hierarchical path, engaging authoritative name servers to retrieve the answer.

Clients can resolve various types of information about the Internet using DNS. This information is encoded in DNS Resource Records (RRs), standardized by the Internet Assigned Numbers Authority (IANA). For instance, clients can query `A` records to obtain the IPv4 address of a specific domain or `NS` records to identify authoritative name servers. With the standardization of Service Binding (SVCB) RRs [16], DNS can now publicly convey even structured, key-value encoded information. In particular, *SVCB* RRs provide clients with additional service information by providing public key material (e.g., in the case of TLS Encrypted Client Hello (ECH) [17]) or additional HTTPS endpoint information such as protocol or port specification, minimizing transient connections to suboptimal servers [16]. DDR leverages SVCB records to provide DNS servers and clients with a predefined schema for exchanging information about DoE endpoints. The DDR protocol is executed as follows (see Figure 2).

1) DDR Discovery with SVCB Records: A DNS client (e.g., stub resolver) is configured with a default recursive resolver IP address. It issues an SVCB query for the special-use domain name `_dns.resolver.arpa`[1] using plaintext DNS. If the recursive resolver has configured DDR, it will return its designated resolvers including their available DoE configuration parameters within the SVCB record(s). For example, Google's popular recursive resolver `8.8.8.8` designates their clients to `dns.google.` while indicating support for DoT and DoT (see second step in Figure 1). Additionally, it provides information about the URI path necessary for DNS queries in DoH. In case DDR is not configured, the server returns an empty set of SVCB records, indicating that it recognizes DDR but has either not implemented the configuration or does not have any designated resolvers. The term *Designated* essentially refers to DoE-enabled resolvers managed by the same entity such as those accessible via the same IP address [15]. DDR-enabled resolvers are referred to as *Designating resolvers*.

2) Selection and Validation of Designated Resolvers: The client may select the designated resolver based on the assigned priority. It then forms an Application-Layer Protocol Negotiation (ALPN) intersection set of the DoE protocol advertised and the protocol(s) the client supports. The selection of the appropriate protocol connection should be made by choosing the higher-priority protocol alternatives and only resorting to the lower-priority options as a fallback if the more preferred transports fail to connect. In case multiple SVCB records share the same priority value within a RR set, clients should randomly select a candidate transport within the same priority level. Moreover, the client utilizes configuration parameters like the `port` value defined in the SVCB record to establish a connection with the DoE endpoint. The DDR-enabled resolver can also indicate the IP addresses of DoE resolvers (`ipv4hint`, `ipv6hint`) to minimize round-trip times for additional name resolving. Finally, the client must verify the authenticity of the selected designated resolver. To this end, the DDR specification defines the process of *Verified Discovery* [15] but leaves additional authentication methods such as policies or heuristics up to the client.

3) Verification & Upgrade to Encrypted DNS: Once the client selects the preferred DoE endpoint, it initiates a TLS handshake, as all DoE protocols are built on top of TLS. The client then proceeds to verify the chain of certificates up to a trust anchor. DDR's *Verified Discovery* further requires the client to verify that the IP address of the DDR-enabled resolver appears in the certificate presented by the DoE endpoint. Specifically, the IP address must be included in the certificate's `subjectAltName` extension. If this check fails, clients are prohibited from upgrading to the DoE endpoint. The *Verified Discovery* mitigates the risk of malicious actors to designating clients to arbitrary DoE endpoints. If the certificates are valid and the authentication process is successful, the client may then use the designated resolver for subsequent encrypted DNS queries.

II. Related Work

Extensive research on large-scale DNS measurements ranges from on-path DNS interception [18], to classic DNS poisoning attacks that enable the manipulation of arbitrary DNS zones [19], and malformed DNS configurations [20], which reveal that large populations of vulnerable systems remain inadequately protected by security mechanisms. This underscores the importance of deploying encrypted DNS communication. Recent studies extensively investigate the adoption of encrypted DNS protocols such as DoT, DoQ, and DoH, highlighting various aspects of their implementation and performance. In the context of server-side availability of DoT and DoH, [21] quantifies the use of DNS privacy behind recursive resolvers. Invalid TLS certificates can be found in encrypted DNS recursive resolver deployments [22], even in university environments [23]. [6] conducted the first comprehensive survey on DNS encryption techniques, highlighting the benefits and limitations of DoE protocols.

[1] Note that `resolver.arpa` remains a local DNS zone outside of the public DNS hierarchy. As a result, security mechanisms such as DNSSEC are not applicable.

They note that while DoT and DoQ offer privacy and performance benefits, they are not widely recognized by security systems and may be blocked by firewalls, whereas DoH is more popular due to its ability to blend with regular HTTPS traffic. The study also discusses the potential for data monopolization and the impact of DoE on ad-blocking efficacy and data exfiltration. With internet-wide scans including 122,991 Vantage Points (VPs) across 166 countries to discover DoE service providers, [24] identify security issues, revealing that 25% of DoT providers use invalid TLS certificates. [25] examine the impact of DoE on DNS manipulation and censorship, finding that more than two-thirds of DoT and DoH resolvers manipulate DNS responses. Their study involve 7.4 million DNS lookup measurements from various VPs. [26] focus on the performance of DoH and DoT, showing that these protocols can be faster than traditional unencrypted DNS under certain network conditions. [10] identify 1,302 operational DoE domains through a 15-month scan utilizing around 5 thousand VP, quantifying and qualifying DoE query blocking. Additionally, they highlight the need for improved DoE discovery methods, such as DDR. [27] are the first to examine SVCB records in the context of HTTPS endpoints. However, they do not cover the DDR specification, which has been standardized to overcome previous DoE discovery and upgrade limitations for clients. Moreover, studies that try to capture a precise image of the current adoption of DoE endpoints use default parameters like ports to probe DoE endpoints [10]. DDR allows as a complementary approach to also capture those DoE resolvers that are outside of standard configurations.

III. Methodology

To assess the adoption of DDR across DNS servers, we develop a three-stage measurement methodology. In the first stage, we collect responsive IPv4 and IPv6 DNS server addresses. In the second stage, these addresses are used to discover DDR resolvers, their DDR configuration and their advertised DoE endpoints. In the third stage, we query these DoE endpoints in their advertised configuration. Finally, we augment the collected dataset with Autonomous System (AS) related data.

1) DNS Server Discovery: To gather IPv4 DNS resolvers, we performed a large-scale DNS scan, from a single VP within an educational network. We used the *ZMap* [28] network scanner to identify IPv4 addresses of publicly available DNS servers that respond on UDP/53. This measurement scans the entire IPv4 address space during July 12th to July 13th of 2024 (1 day and 17 hours) with a probe file querying the IPv4 address of `www.google.com`. The result set includes all IPv4 addresses that responded to the probe, including those issuing a DNS reply with *RCODE* 5, thereby refusing to answer the query. In total, the scan produced a list of 27 060 938 IPv4 addresses. To minimize the impact of IP address churn [29], we pipe the IPv4 addresses to the DDR discovery scanner directly once an IP address was found by *ZMap*. To cover the IPv6 address family as well, we collect UDP/53 responsive DNS servers from the *IPv6 Hitlist Service* [30], [31], [32]. We use their latest scan from July 15th of 2024 which contains 419 064 IPv6 addresses. The IPv6 scan was conducted on 21st of July 2024.

2) DDR Discovery: To discover DDR-enabled DNS servers, we implemented a tool that sends dedicated DDR discovery queries to a set of IP addresses and parses the DDR response. We set a timeout of 2.5 seconds for each DDR query's lifetime. Moreover, we implement a retry strategy: We attempted at most three times on UDP/53. After three unsuccessful queries on UDP/53, we query once on TCP/53. We also consider the fallback mechanism of DNS to TCP in case the truncation bit (TD) is set [33]. The tool further isolates all the successful DNS responses, parses them and outputs a list of DoE endpoints including their configuration.

3) DoE Resolver Probing: We use the list of DoE endpoints to probe for an `A` wildcard record within our own DNS zone, with a timeout set to 5 seconds. This enables the crafting of uniquely identifiable DNS queries, distinguishable both at the scanner and our authoritative name servers. To minimize network traffic and potential negative impacts on the encrypted resolvers, each resolver is queried only once. Additionally, we account for specific implementation details of all DoE protocols. For instance, with DoH, a fallback to `POST` HTTP requests is necessary if the queried URL exceeds the 255-character limit, shifting the encoded DNS query to the body of the HTTP request [11].

4.) Data Enrichment with AS-related Information: To analyze the adoption of DDR by various network types, we first map the IP addresses to ASes by using *GeoLite2* [34]. To identify which type of networks offer more support for DDR, we make use of PeeringDB's [35] `info_type` classification (see Table I). This classification groups ASes in network types: Cable/DSL/ISP (such as Vodafone), Content (such as Netflix), Enterprise (such as Tesla), Educational/Research (such as China Education and Research Network), Network Service Provider (NSP) (such as IONOS SE), Route Servers (such as MSLINK), Non-Profit (such as PARKNET), and Government (such as Justica Federal de Primeiro Grau no RS). For simplicity, we merge Route Server and Route Collector as the same network, and Network Services and NSP as the same network, respectively.

A. Artifacts

To foster reproducibility and support further research, both the measurement tool *DoE-Hunter* [36] and the associated dataset [37] have been made publicly available online.

B. Ethical Considerations

We follow best practices to ensure ethical research, focusing on publicly resolvable DNS data without collecting personal information or exploiting insecure systems. By using well-established scanning tools such as *ZMap* [28] and data from the *IPv6 Hitlist Service* [30], [31], [32], we ensure that our measurements do not congest networks. For instance, *ZMap* employs a permutation approach, which randomly selects IP addresses to scan rather than following a sequential numerical order, thus preventing concentrated network load [28]. We implement a caching mechanism to prevent multiple queries for the same DoE resolver, thereby reducing unnecessary traffic. Our scanner nodes and name servers are configured for transparency, including relevant `TXT` records and reverse DNS entries linking to our measurement approach and contact information. Finally, the scanner nodes operate within an academic network, where responsible system administrators are informed of our measurement activities.

IV. Analysis

In total, we discovered 27 480 002 responsive resolvers covering 46 392 ASes (see Table I) which we subsequently scanned for DDR discovery. These DDR responses include SVCB records indicating support for DoE protocols such as DoT, DoH/1.1, DoH/2, DoH/3, and DoQ, originating from a total of 301 780 unique resolvers out of 4 091 519 correctly responding servers, distributed across 15 900 ASes (34.27 % of the ASes in our dataset). We observe that 99.41%

of DDR-enabled resolvers are recursive resolvers, as indicated by the Recursion Available (RA) bit in their corresponding DNS responses.

A. DNS Dataset

The DNS servers are spread over a wide spectrum of ASes, ranging from ASes with a minimum of one resolver to a maximum of more than 8M DNS resolvers inside one network (AS4837, China Unicom). However, intriguingly, only 1051 (1033 IPv4 and 18 IPv6) of the DNS resolvers within China Unicom appear to offer support for DDR. Around 42 % of the networks do not reveal network-type information in PeeringDB (empty `info_type` value). Among the rest 58 %, 42 % resolvers are deployed inside NSP networks, 11% belong to content providers, enterprise and cloud providers constitute around 1 %, and 0.5 % resolvers belong to educational networks (see Table I). Furthermore, a substantial proportion of these prominent ASes are concentrated in the Asian region spread across various network types, but the majority lies within ISPs such as China Unicom, Chinanet (NSP), China Education and Research Network (Education), Korea Telecom (ISP) and Alibaba (Content). Notably, our dataset prominently features one major content provider: the Alibaba Group (AS37963) contributing with 1 132 568 (4.13 %) to the overall dataset of found DNS resolvers. In contrast, Microsoft (AS8075) has 10 109 resolvers, representing 0.036 % overall. Around 1.24 % of all resolvers are associated with enterprise networks, of which Amazon dominates. Within educational and research networks, a substantial portion is attributed to the China Education and Research Network (AS4538) and Consortium GARR (AS137). They alone account for 76 % of the total number of resolvers of educational ASes. Overall, 15 964 769 (58.19 %) of the DNS resolvers in the dataset appear to be located in China alone.

B. DDR Adoption

Only considering the 27 060 938 IPv4 DNS servers, 292 260 (1.08 %) resolvers advertised DDR, 3 712 317 (13.72 %) returned no DDR configuration. The remaining 23 056 361 (85.20 %) servers either refused the request, ran into a timeout or returned an error. As a result, 7.30 % of the correctly responding DNS resolvers in IPv4 offer a DDR configuration. Interestingly, the ratio between servers that have not configured DDR and servers whose DDR queries failed is significantly different from IPv4 in the IPv6 address space: Of the 419 064 IPv6 DNS servers scanned, 9520 (2.27 %) servers have DDR configured, while 379 202 (90.49 %) lack a configuration. In contrast to IPv4 resolvers, only 30 342 (7.24 %) servers failed or refused to respond to the DDR query. Therefore, a total of 2.51 % of the reliable IPv6 resolvers are equipped to support DDR.

TABLE I
Total number of scanned DNS resolvers for DDR discovery grouped by their AS network type in relation to the resolvers that advertise DDR. The DDR adoption column shows the DNS-supported servers while the percentage shows the adoption rate of DNS servers that responded without any errors, i.e., DDR compliant DNS servers.

Network Type	# DNS Resolver ↓	# Total ASes	DDR Adoption	# DDR ASes
unkown	11,600,414 (42.21%)	31,392 (67.67%)	111,585 (8.83%)	8,479 (53.32%)
NSP	11,479,409 (41.77%)	3,206 (6.91%)	68,537 (8.21%)	1,699 (10.68%)
Content	3,039,289 (11.06%)	1,428 (3.08%)	9,584 (0.62%)	393 (2.47%)
Cable/DSL/ISP	881,744 (3.21%)	8,564 (18.46%)	107,002 (17.65%)	4,966 (31.23%)
Enterprise	340,106 (1.24%)	805 (1.74%)	2,705 (3.58%)	179 (1.13%)
Ed./Research	131,772 (0.48%)	587 (1.27%)	1,726 (3.11%)	130 (0.82%)
Non-Profit	6,192 (0.02%)	315 (0.68%)	345 (6.61%)	42 (0.26%)
Government	599 (<0.01%)	67 (0.14%)	21 (4.17%)	7 (0.04%)
Route Server	477 (<0.01%)	28 (0.06%)	275 (70.33%)	6 (0.04%)
Total	27,480,002	46,392	301,780	15,901

TABLE II
Top 10 networks (ASes) with the largest number of DNS resolvers supporting DDR discovery.

	AS	Organization	# DDR ↓ resolvers	Network Type
		IPv4		
1	36994	Vodacom-VB	6,900 (2.36%)	NSP
2	17488	Hathway IP Over Cable Internet	4,460 (1.53%)	Cable/DSL/ISP
3	58224	TC Iran	4,086 (1.40%)	unkown
4	7713	PT Telekomunikasi Indonesia	3,345 (1.14%)	NSP
5	22773	Cox Communications	2,244 (0.77%)	Cable/DSL/ISP
6	16637	MTN Business Solutions	2,099 (0.72%)	NSP
7	8151	UNINET	1,986 (0.68%)	NSP
8	9299	PLDT	1,953 (0.67%)	NSP
9	7922	Comcast Cable Communications	1,814 (0.62%)	Cable/DSL/ISP
10	4134	Chinanet	1,814 (0.62%)	NSP
		IPv6		
1	27839	Comteco Ltda	4,245 (44.59%)	Cable/DSL/ISP
2	6939	Hurricane Electric	356 (3.74%)	NSP
3	266423	Connectvy Telecomunicacoes	294 (3.09%)	NSP
4	1929	UMass NET	168 (1.76%)	unkown
5	263762	Coopeguanacaste	130 (1.37%)	Cable/DSL/ISP
6	16276	OVHcloud	123 (1.29%)	Content
7	201565	Etruria Wi-fi S.r.l.	111 (1.17%)	unknown
8	44489	STARNET, s.r.o.	85 (0.89%)	Cable/DSL/ISP
9	14061	Digital Ocean	81 (0.85%)	Content
10	8966	Etisalat	76 (0.80%)	NSP

TABLE III
The top five DoE endpoints to which clients are redirected via DDR, categorized by network type and DoE endpoint domain.

	Network Type	Designation	Occurrences ↓
		IPv4	
1	unkown	`dns.google.`	93,720 (85.33%)
2	Cable/DSL/ISP	`dns.google.`	80,546 (79.83%)
3	NSP	`dns.google.`	47,341 (78.08%)
4	Cable/DSL/ISP	`one.one.one.one.`	11,997 (11.89%)
5	NSP	`one.one.one.one.`	9,844 (16.24%)
		IPv6	
1	Cable/DSL/ISP	`dns.google.`	5,622 (92.09%)
2	NSP	`dns.google.`	1,099 (74.86%)
3	unkown	`dns.google.`	894 (79.89%)
4	Cable/DSL/ISP	`one.one.one.one.`	277 (4.54%)
5	Content	`dns.google.`	269 (47.19%)

Table I shows the distribution of DDR-enabled resolvers by network type. It can be seen that a large number of resolvers with DDR support are located inside ISP networks (107 002). However, this is still a comparably small proportion of overall ISP resolvers with DDR support, with merely 12 % of these ISP resolvers embracing DDR and around 18 % only considering those servers that responded without any errors. In contrast, 70.33 % of the servers categorized as route server advertise DDR which makes around 70 % only considering non-error returning servers. Finally, DDR adoption is notably sparse in content networks, with just 0.62 % of the resolvers. This highlights the very limited adoption of resolvers that offer support for DDR, as of July 2024.

Table II shows the list of the top ten ASes of IPv4 and IPv6 ordered by the number of DDR-enabled resolvers within the AS, demonstrating that a large proportion of DDR-enabled resolvers are located inside ISP and NSP networks compared to other network types. In fact, around 72 % of DDR-enabled resolvers can be located in ISP and NSP network types.

TABLE IV
DOE PROTOCOLS OF DESIGNATED RESOLVERS ADVERTISED BY THE DDR-SUPPORTED RESOLVERS DEPENDING ON THE NETWORK TYPE.

Networks↓	**# DDR ↓ resolvers**	**DoH/1.1 (%)**	**DoH/2 (%)**	**DoH/3 (%)**	**DoT (%)**	**DoQ (%)**
unkown	111,585	0.82	99.98	95.29	99.78	1.04
Cable/DSL/ISP	107,002	0.20	99.96	92.92	98.38	0.42
NSP	62,096	0.25	99.97	95.04	99.76	0.50
Content	9,584	0.21	99.47	86.23	94.04	6.02
Network Services	6,441	0.09	99.98	97.55	99.91	0.19
Enterprise	2,705	0.11	99.96	90.13	98.82	1.33
Ed./Research	1,726	0.06	100	68.25	99.77	0.29
Non-Profit	345	0.29	100	98.26	100	0.29
Route Server	275	0	100	100	100	0
Government	21	0	100	95.24	100	0

TABLE V
TOP 10 (OUT OF 1,277) ADVERTISED UNIQUE ALTERNATIVE DOMAINS AND DOE PROTOCOLS OF DDR-SUPPORTED RESOLVERS.

Domains	**DoH/1.1**	**DoH/2**	**DoH/3**	**DoT**	**DoQ**
`dns.google.`	-	245,651	245,651	245,654	-
`one.one.one.one.`	-	34,905	34,905	34,905	-
`dns.umbrella.com.`	-	8,509	-	8,511	-
`dns.opendns.com.`	-	8,510	-	8,509	-
`doh.opendns.com.`	-	8,376	-	-	-
`doh.umbrella.com.`	-	8,375	-	-	-
`dns.quad9.net.`	-	3,819	-	3,819	-
`familyshield.opendns.com.`	-	3,013	-	3,013	-
`dns.adguard-dns.com.`	849	849	849	849	849
`doh.familyshield.opendns.com.`	-	3,013	-	-	-
Total	**1,309**	**330,039**	**283,563**	**307,650**	**2,646**

We observe that DDR-enabled resolvers represent a very small proportion (up to 2.36 %) within each AS category in IPv4. Vodacom-VB - a large NSP owned by Vodafone and Telkom located in South Africa - appears to host the largest number of resolvers that support DDR representing 2.36 % of the total IPv4 DDR-enabled resolvers. Surprisingly, they do not host any IPv6 DDR-enabled resolvers in any of their ASes as observed in our dataset. In the case of IPv6, almost half of the DDR resolvers are part of the AS27839 (Comteco Ltda) although responsive UDP/53 addresses show an uniform distribution among ASes in the *IPv6 Hitlist Service* [31]. Further, we can only observe content providers (OVHcloud and Digital Ocean) in the top ten IPv6 networks, with no content provider making it to the list of IPv4 networks. Among the content providers that support DDR in IPv4, LayerHost (AS46573) provides the largest amount of resolvers with 991 (0.34 %) in total. In contrast, Google (AS15169) presents a relatively modest count of 16 DDR-enabled resolvers in general, constituting only 0.002 % of the total DDR-enabled resolvers in the category of content providers. Similarly, Cloudflare (AS13335) operates a total of 27 DDR-enabled resolvers.

A notable trend throughout all network types is the tendency for approximately 93 % of DDR-enabled resolvers to designate clients to major cloud DNS service providers: 81 % (84 % IPv6) of them designate to Google (`dns.google.`), while 12 % (9 % IPv6) designate to Cloudflare (`one.one.one.one.`). Table III shows that especially ISPs tend to redirect their customers to Google or Cloudflare, while both make up to 97 % of all advertised encrypted resolvers. Note that in Table III, a DDR resolver may provide a designation multiple times, leading to multiple counts in this listing. The percentage represents the proportion of occurrences within the same network type. Overall, the observed pattern of centralization raises concerns about potential privacy risks and aligns with previous research on the challenges of cloud adoption [38]. This contrasts sharply with the concept of DDR, which aims to preserve user privacy [15] by enabling the automatic discovery of designated (DoE) resolvers.

C. DoE Protocol Distribution

DoE protocols are available in five different flavors, each represented by ALPN values in SVCB resource records sent by DDR-enabled resolvers, as shown in Table IV. These variants include: DoH/1.1, DoH/2, DoH/3, DoT, and DoQ. We evaluate the popularity of these protocols when DDR-enabled resolvers designate clients to third party DoE resolvers, also known as alternative domains. Table IV presents the proportion of each DoE protocol advertised by the DDR-resolvers across different network types. It is noteworthy that among all network types almost every DDR-resolver offers a DoE resolver with DoH/2 support, while the adoption of DoQ remains low at a median of 0.36 %. Furthermore, we notice that DoT and DoH/2 are the most widely adopted DoE protocols supported by almost 98 % of the advertised DoE resolvers. Among the top 10 most advertised DoE resolvers, only `dns.adguard-dns.com` (AdGuard DNS) has support for all four DoE protocols standardized by the IETF. Notably, only 2500 (0.83 %) DDR-enabled resolvers designate clients to use DoQ for encrypted DNS, despite previous studies demonstrating DoQ's improved performance and privacy benefits over other DoE protocols [39]. However, DDR-enabled resolvers inside content-based networks provide the highest level of support for DoQ. In 32.09 % of the cases, the most prominently advertised DoQ resolver is `dns.adguard-dns.com`, which has a total of 849 listings. Interestingly, 2.61 % (62) of the overall DoQ endpoints target to "`.`". This redirection target is defined in DDR's underlying specification [40] and expresses a redirection to the same host. This configuration is prohibited by the DDR specification [15] which results in clients dropping this configuration and falling back to unencrypted DNS if no other DoE protocol is offered. Also, neither Google (`dns.google.`) nor Cloudflare (`one.one.one.one.`) offer DoQ through DDR although they make up to 93 % of the total designated resolvers. A possible explanation for the low adoption rate of DoQ in general is the lack of implementation and support for DoQ in widely used DNS server software, such as *BIND* or *Microsoft DNS*. In contrast to DoQ, DoH/1.1 is 1306 times advertised (0.43 %) which demonstrates an intent to keep support for legacy encrypted DNS protocols as well.

The overall support for DoH/3 is relatively high, with a median of 95.14 %, despite its reliance on QUIC as an underlying transport protocol, similar to DoQ. Educational networks exhibit the lowest proportion of DoH/3 resolvers at only 68.25 %, but conversely, they also have one of the lowest proportions of the legacy DoH/1 support (0.06 %). Regarding route servers, three key observations emerge: First, they demonstrate the highest adoption of DDR among all network types, with a rate of 70.33 % (see Table I). Second, route servers that support DDR invariably offer DoH/2, DoH/3, and DoT, but never DoQ. Finally, these servers consistently designate to either Google or Cloudflare as their encrypted DNS providers (see Table VI).

D. Leaking Privacy to Cloud Providers

A DDR-enabled resolver can technically designate clients to a third party that handles the client's subsequent encrypted DNS requests. These third parties, known as alternative domains, effectively refer to a DoE resolver. Table VI shows the popularity (top 10) of such alternative domains on the basis of the number

TABLE VI
THE POPULARITY OF TOP 10 (OUT OF 1,277) ALTERNATIVE DOMAINS DESIGNATED BY THE RESOLVERS INSIDE VARIOUS NETWORKS (IPV4 AND IPV6 DDR SERVER COMBINED). NOTE THAT A DDR DISCOVERY CAN RESPOND WITH A LIST OF MULTIPLE ALTERNATIVE DOMAINS.

Domain	**Network Type**								
	Cable/DSL/ISP	**Content**	**Ed./Research**	**Enterprise**	**Government**	**NSP**	**Non-Profit**	**Route Server**	**unkown**
`dns.google.` (736,956)	258,510 (78.88%)	19,340 (66.52%)	3,063 (57.56%)	6,000 (72.52%)	42 (66.67%)	162,555 (77.26%)	936 (89.4%)	801 (97.09%)	285,709 (83.43%)
`one.one.one.one.` (104,715)	36,840 (11.24%)	5,196 (17.87%)	375 (7.05%)	1,176 (14.21%)	12 (19.05%)	31,809 (15.12%)	63 (6.02%)	24 (2.91%)	29,220 (8.53%)
`dns.umbrella.com.` (17,020)	7338 (2.24%)	782 (2.69%)	110 (2.07%)	230 (2.78%)	0	3688 (1.75%)	8 (0.76%)	0	4864 (1.42%)
`dns.opendns.com.` (17,019)	7,336 (2.24%)	782 (2.69%)	110 (2.07%)	230 (2.78%)	0	3,690 (1.75%)	8 (0.76%)	0	4,863 (1.42%)
`doh.opendns.com.` (8,376)	3,645 (1.11%)	391 (1.34%)	55 (1.03%)	67 (0.81%)	0	1,805 (0.86%)	4 (0.38%)	0	2,409 (0.7%)
`doh.umbrella.com.` (8,375)	3,645 (1.11%)	391 (1.34%)	55 (1.03%)	67 (0.81%)	0	1,805 (0.86%)	4 (0.38%)	0	2,408 (0.7%)
`dns.quad9.net.` (7,638)	2,780 (0.85%)	618 (2.13%)	34 (0.64%)	126 (1.52%)	0	1,696 (0.81%)	4 (0.38%)	0	2,380 (0.69%)
`familyshield.opendns.com.` (6,026)	1,464 (0.45%)	22 (0.08%)	938 (17.63%)	112 (1.35%)	2 (3.17%)	740 (0.35%)	0	0	2,748 (0.8%)
`dns.adguard-dns.com.` (4,245)	650 (0.20%)	75 (0.26%)	5 (0.09%)	10 (0.12%)	0	525 (0.25%)	5 (0.48%)	0	2975 (0.87%)
`doh.familyshield.opendns.com` (3,013)	732 (0.22%)	11 (0.04%)	469 (8.81%)	56 (0.68%)	1 (1.59%)	370 (0.18%)	0	0	1374 (0.40%)

of DDR-enabled resolvers that choose to redirect to these third-parties.. For instance, more than 99 % of the resolvers inside the ISP networks redirect their clients to either of these top 10 cloud DNS providers for handling subsequent encrypted DNS requests, while `dns.google.` alone accounts for approximately 79 %. It can clearly be seen that amongst all network types, Google DNS is by far the most advertised designated resolver, ranging from 58 % in educational (or research) networks to 97% in route server networks. However, in educational networks, there is a trend to designate to `familyshield.opendns.com.` (18 %) which is a service offered by OpenDNS provided by Cisco to block explicit content. Ordered by proportion within the network types, the unencrypted resolvers within content delivery networks also have the most designations to `dns.quad9.net` (around 2 %), a service offered by Quad9. It is worth noting that the top ten alternative domains show only negligible differences between IPv4 and IPv6 DDR-enabled resolvers across network types. Table V highlights the pivotal role of cloud DNS services in combination with the advertised DoE protocols. Again, more than 85 % of the DDR-enabled resolvers designate to Google DNS, i.e., redirected to a third party, outside of the boundary of the AS from where the DDR discovery request originates. The centralization of DNS traffic poses not only privacy concerns but also legal and political implications that could impact the digital sovereignty of countries [41], [42].

In summary, we underline two key points: First, while designated DoE resolvers effectively protect DNS communication from eavesdroppers, they still expose the client's DNS queries to third-party resolvers. Second, our findings highlight the significant influence cloud service providers have on the adoption of DoE protocols from the viewpoint of DDR. For instance, if Google DNS were to offer DoQ via DDR, assuming the DDR configurations were adjusted accordingly, we would likely observe a rapid increase in DoQ adoption.

E. Priority of Encrypted DNS Protocols

We further assess the support for various DoE protocols based on the alternative domains reported by DDR-enabled resolvers. Our findings show that DoH/2 is the most widely advertised, appearing in 99.95 % of all DDR resolvers, followed by DoT (99.09 %), DoH/3 (93.96 %), DoQ (0.84 %), and DoH/1.1 (0.43 %). DDR-enabled resolvers offer 9 combinations of these DoE protocols. We examine the popularity of protocol combinations offered via alternative endpoints of DDR-enabled resolvers. The most common combination — (DoT, DoH/2, DoH/3) — is offered by 93.51 % of resolvers, followed by (DoT, DoH/2) at 5.10 %. All other combinations, including those involving DoH/1.1 and DoQ, appear in less than 1 % of cases. Notably, the legacy protocol DoH/1.1 and the newer DoQ share similarly low adoption rates. Among the rare occurrences of DoQ, it is most often paired with DoH/2, appearing in 0.82 % of cases.

Each advertised DoE resolver and its associated protocols are assigned specific priorities. This prioritization allows the DDR-enabled resolver to indicate preferences, thereby guiding clients on which designated resolver to use. The higher the priority, the more preferred the protocol is for the client to follow. We observe that DoQ consistently holds the lowest priority among all DoE protocols assigned by each DDR resolver. Again, this is surprising, considering recent studies have demonstrated the privacy and performance advantages of DoQ over DoT [39], [43]. Moreover, when comparing the priority between DoQ and DoH/3, which also uses QUIC as an underlying protocol, DoH/3 is prioritized higher in 95 % of all cases. This contrasts with the DoQ standard [13], which suggests that DoQ provides a more lightweight alternative to DoH by eliminating the overhead associated with HTTP.

There are instances where protocols are assigned the same priority. For example, DoQ and DoH/3 share the same priority in 0.02 % of the instances (68 times), while DoH/3 and DoH/2 share priorities in more than 93 % (283 563 times). In such cases, the specification suggests that clients apply a random shuffle within a priority level to the records before using them to ensure uniform load-balancing of encrypted DNS queries [40]. Further, for all the combinations with DoH/1.1, the protocol has the highest priority in every case and is always offered alongside DoH/2 and DoH/3. Notably, only two entities provide this combination: AdGuard, with 216 different encrypted resolvers using this protocol permutation, and ControlD - a service offering customizable DNS-based content filtering - with 2 different encrypted resolvers.

An analysis of all protocol combinations reveals that DoT is assigned the highest priority in 86.55% of cases, followed by DoH/2 (13.45 %), DoH/3 (12.55 %), DoH/1.1 (0.43 %), and DoQ (0.40 %). This indicates that DoT is the most commonly prioritized DoE protocol. However, despite its widespread prioritization, DoT operates on a dedicated port (853), and prior studies have shown that such traffic is frequently dropped by middleboxes, potentially disrupting encrypted DNS communication and undermining the resiliency of the protocol [10].

F. Routing and Non-Standard Ports

The number of SVCB resource records' parameters varies across all DDR-enabled resolvers. Some resolvers respond with five different parameters including `ipv6hints` and `ipv4hints` (see: Section I-A1 for preliminaries), while others provide most commonly only one parameter which is `alpn`. Approximately 77 % of the DDR resolvers do not offer either `ipv4hints` or `ipv6hints`.

TABLE VII
THE POPULARITY OF TOP 10 (OUT OF 27) ALTERNATIVE DOMAINS DESIGNATED BY THE RESOLVERS ADVERTISING A NON-DEFAULT QUERY PATH.

	Domains	Path	Occurrences ↓
1	`dns.controld.com.`	`/comss{?dns}`	18 (22.22%)
2	`dns0.eu.`	`/`	11 (13.58%)
3	`dns.controld.com.`	`/{?dns}`	8 (9.88%)
4	`freedns.controld.com.`	`/p2{?dns}`	7 (8.64%)
5	`zero.dns0.eu.`	`/`	4 (4.94%)
6	`freedns.controld.com.`	`/uncensored{?dns}`	3 (3.7%)
7	`open.dns0.eu.`	`/`	3 (3.7%)
8	`dns.jamessilu.com.`	`/dns-query?dns`	2 (2.47%)
9	`doh.ticklers.org.`	`/dns{?dns}`	2 (2.47%)
10	`dns.controld.com.`	`/2adace8hybt{?dns}`	2 (2.47%)

We suspect these resolvers prefer to use DNS alternative names (such as `dns.google.`) to redirect clients to the nearest Google DNS replica that can serve the encrypted DNS request. Meanwhile, few default resolvers advertise just one IPv4 address (only 34, <0.01 %), whereas 20 % advertise only one IPv6 hint. In the case of IPv4, we suspect these are anycasted IP endpoints (such as `1.1.1.1`) whereby the designated resolver resorts to Border Gateway Protocol (BGP) for similar redirections to the nearest replica, instead of using DNS. Otherwise each address family is configured with a maximum of two IP addresses to allow a client to fallback if the primary endpoint fails to connect.

Another method of mitigating circular DNS resolution and network latency is to append so-called glue records (additional to `ipv4hint` or `ipv6hint`). These records are additional entries attached to a DNS response and can contain `A` or `AAAA` records for the IPv4 and IPv6 addresses of the advertised encrypted resolvers. Note that clients may still ignore these because they are out-of-bailiwick [44]. 60 % of the DDR-enabled resolvers attach those glue records for their advertised encrypted resolvers while 91 % of the glue records contain IPv4 addresses and 87 % contain IPv6 addresses. 87 % of the DDR resolvers offer both IP hints and glue records simultaneously.

Interestingly, we observe that some designated resolvers offer DoE protocols on non-standard ports such as 3443 instead of port 443 for DoH traffic. This appears to reflect a *security by obscurity* strategy, based on the assumption that malicious actors often target default ports. We observe port deviation from these default protocol ports in 0.11 % of the advertised DoE resolvers, and this deviation is only detectable when either DoQ or DoH/2 is advertised. Among the 1203 unique encrypted resolvers offering DoQ, 13.63 % deviate from the default port 853, with the majority (80.49 %) using port 784 instead. In contrast, 1189 of the unique encrypted resolvers offering DoH/2, 29.43 % use non-standard ports, with 21.14 % of these instances using port 8443.

G. DoH Paths and ODoH

According to [16], an encrypted resolver offering DoH must specify the URI path for encrypted DNS queries. Our analysis confirms that all encrypted resolvers supporting DoH include the `dohpath` parameter, with 97.69% using the standard path `/dns-query?dns` as defined in [16].

Table VII presents alternative DoH paths that deviate from the specification outlined in [16], organized by their frequency of occurrence. Two notable patterns emerge: First, similar to the deviation in ports, some paths appear to employ *security by obscurity*, with paths seemingly chosen at random (see the 10th entry in Table VII). Second, approximately 25% of the deviating paths are non-compliant with [16], as they do not include the mandatory `dns` variable. This non-compliance prevents clients from parsing the DoH path, causing them to ignore the offered resolver and, in the worst case, fall back to unencrypted DNS.

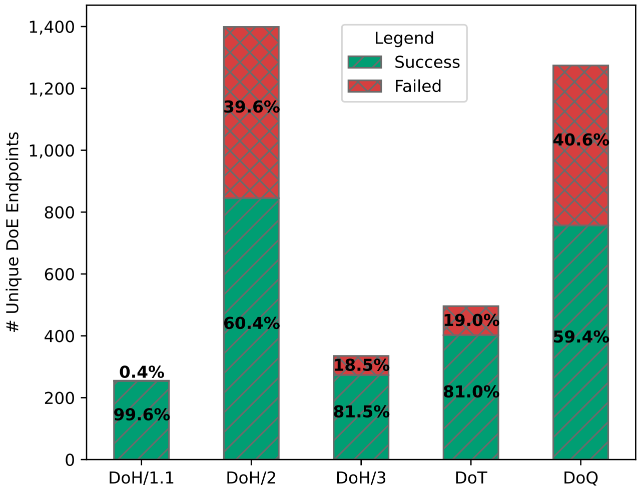


Fig. 3. The query success rate of the unique DoE endpoints from the resulting DDR discovery of the 301,780 DDR-supported resolver in our dataset.

Although a client may use DoE for its DNS queries, the DoE resolver still observes the client's IP address. To address this privacy concern, Oblivious DNS over HTTPS (ODoH) was standardized in mid-2022 [45]. Essentially, ODoH enables encrypted DNS queries to be routed through a proxy, ensuring that the encrypted resolver only observes the proxy's IP address, thereby concealing the client's identity. DDR supports the discovery of ODoH endpoints [46]. Noteably, we could not observe a single DDR-enabled resolver offering ODoH. For instance, although Cloudflare offers both ODoH [47] and DDR, their DDR configuration does not contain their ODoH encrypted resolver. This discrepancy indicates a mismatch between observed DDR configurations and the actual configurations of encrypted resolvers.

H. DoE Endpoint Analysis

The DDR measurement yields 3759 unique encrypted resolvers. We query these encrypted resolvers with an `A` query probe on our own domain, using a timeout of five seconds. As illustrated in Section IV-H, 33.84 % of the queries failed across all DoE resolvers, which is a cause for concern. Among the unique DoE resolvers, we identify the highest counts for DoQ (1399) and DoH/2 (1274) resolvers. This is a noteworthy observation, as DoQ is generally the least advertised protocol among all DDR-enabled resolvers (see Table IV), yet it ranks among the most frequently encountered in the set of unique DoE resolvers.

Subsequently, we query 1399 DoH/2, 1274 DoQ, 496 DoT, 335 DoH/3, and 255 DoH/1.1 resolvers. Nearly all queries sent via DoH/1.1 receive successful responses (99.61 %), whereas we observe a notably high failure rate for DoQ (40.58 %) and DoH/2 (39.60 %). Upon examining the causes of DoQ query failures, we find that 17.72 % are due to expired or self-signed certificates. In 69.07 % of cases, the query results in a timeout, and in the remaining 13.38 %, the alternative domain cannot be resolved prior to attempting a connection to the DoQ resolver. Similarly, for DoH/2, 11.85 % of errors result from lookup failures, while 17.15 % are caused by misconfigured certificates, such as expired or self-signed ones. Additionally, 8.93 % of DoH resolvers reject the query with HTTP status codes such as 403. The remaining errors include 11.85 % lookup errors and 27.89 % various other issues, such as connection resets or parsing errors of the DNS response from the resolver. We highlight that the error spectrum for DoH is significantly broader compared to other DoE protocols, with a total of 33 different errors observed. In the case of DoT, the majority of errors are attributable to unreachable hosts, accounting for 70 % of the total errors. Certificate validation failures constitute 15% of the errors, while the remaining 15% are due to DNS resolution issues associated with alternative domains.

The high number of errors is concerning, as errors in the DNS resolution process not only slow down or delay dependent applications but can also result in clients falling back to unencrypted DNS in the worst-case scenario. This corroborates our hypothesis that the configuration of DDR does not always align with the actual deployment and configuration of DoE resolvers.

I. Limitations and Future Work

We derive our DNS dataset from a *ZMap* scan of IPv4 addresses and responsive UDP/53 IPv6 addresses identified by the *IPv6 Hitlist Service* in July 2024. As a result, resolvers inactive during the scan are inherently excluded. The DDR scan is a one-time measurement from a single VP in an educational network, potentially projecting an inaccurate depiction of the DNS landscape. Additionally, approximately 0.17 % of the scanned IP addresses lack AS-related metadata. Furthermore, due to incomplete data in the PeeringDB database, approximately 42 % of DNS resolvers and 37 % of DDR-enabled resolvers cannot be classified into specific network types. Additionally, the categorization of ASes by PeeringDB may be inaccurate; for instance, Google (AS15169) is classified as a content provider, yet it also functions as an enterprise company. This misclassification could potentially introduce bias into the analysis of network types within the broader resolver landscape.

The study does not distinguish between servers lacking DNS and DDR support and those whose responses are dropped (e.g., by a malicious actor en route). As detailed in Section III, we mitigate such effects by querying SVCB records four times (three via UDP, one via TCP), but do not explicitly filter such attacks. Although periodic re-queries are recommended by the specification, this is not implemented in our study.

The timeout durations of 2.5 seconds for the DDR query and 5 seconds for probing discovered DoE resolvers may be insufficient to fully mitigate bias in timeout results. Specifically, 69.07 % of all errors in DoE probes are attributed to timeouts. It remains unclear whether these timeouts are due to resolver unavailability or because the DoE resolver is unable to respond within the given time frame due to the resolution process of our issued DNS query probe (e.g., latency).

Finally, it remains unclear whether clients follow third-party designations outside the same administrative entity (*Verified Discovery* [15]), in part due to limited client-side DDR support (e.g., in systemd-resolved) at the time of writing.

V. Conclusion

We present a large-scale measurement of the DDR protocol across more than 27M DNS servers in the IPv4 and IPv6 address space. Our findings reveal that from around 4M correctly responding DNS servers, 301 780 DNS servers support DDR (7.2 %), with the vast majority being recursive resolvers (99 %). Notably, we find that DoH/2 is the most widely supported encrypted DNS protocol among encrypted resolvers offered by DDR, followed by DoT and DoH/3, while DoQ is rather sparsely offered by only 0.36 % of DDR-enabled resolvers. These observations indicate a disconnect between the operational and scientific communities as recent studies have repeatedly demonstrated that DoQ performs best among DoE protocols with respect to privacy and performance. Significantly, we find that approximately 99% of default resolvers redirect clients to encrypted DNS resolvers that are hosted by large cloud DNS providers like Google, Cloudflare, OpenDNS, or AdGuard. Google and Cloudflare together alone contribute up to 97% of encrypted resolvers advertised by DDR resolvers, amplifying the issue of centralization of data to hyper-giants and raising critical concerns regarding potential privacy leakage of DNS queries to a third party.

We also identify significant variations in the advertised encrypted resolvers, with some resolvers employing non-standard ports and paths, highlighting aspects of encrypted resolvers not covered by recent studies such as [10]. Furthermore, we observe a lack of ODoH indication among DDR resolvers, despite its potential to enhance privacy by preventing the encrypted resolver from learning the client's IP address. The high number of encountered query errors of DDR-discovered DoE resolvers is also concerning, particularly when clients select DoH/2 or DoQ as their preferred DoE protocol. 33.84% of the queries to these encrypted resolvers fail due to various errors such as misconfigured certificates, leading clients to fall back to unencrypted DNS in the worst-case scenario.

Overall, our study presents the first unique perspective on the discovery of designated resolvers protocol and illuminates the privacy repercussions that are associated with the way the protocol is being deployed on the Internet. Our research findings indicate that even in the implementation of encrypted transports in DoE (DoH, DoT, DoQ), there is a concerning centralization around two companies that has an adverse impact on user privacy and the digital sovereignty of countries.

References

[1] S. Bortzmeyer, "DNS privacy considerations," https://doi.org/10.17487/RFC7626, pp. 1–17, May 2015.

[2] D. Herrmann, C. Gerber, C. Banse, and H. Federrath, "Analyzing characteristic host access patterns for re-identification of web user sessions," in *NordSec 2010*, vol. 7127, Finland, 2010, pp. 136–154.

[3] G. C. M. Moura, S. Castro, W. Hardaker, M. Wullink, and C. Hesselman, "Clouding up the Internet: how centralized is DNS traffic becoming?" in *ACM IMC*, ser. IMC '20, 2020, p. 42–49.

[4] F. Le, J. Ortiz, D. C. Verma, and D. D. Kandlur, "Policy-Based Identification of IoT Devices' Vendor and Type by DNS Traffic Analysis," in *PADG@ESORICS 2018*, vol. 11550, Spain, 2018.

[5] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic," 2017.

[6] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques," *ACM Comput. Surv.*, vol. 55, no. 8, 2023.

[7] C. Chan, R. Fontugne, K. Cho, and S. Goto, "Monitoring TLS adoption using backbone and edge traffic," in *IEEE INFOCOM 2018*, 2018.

[8] M. Trevisan, D. Giordano, I. Drago, M. M. Munafò, and M. Mellia, "Five Years at the Edge: Watching Internet From the ISP Network," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 561–574, 2020.

[9] Q. Chen, Y. Zhuang, J. Liang, J. Hai, and D. Hou, "Research on DNS Encryption Technology," in *Conference on Computer Engineering and Networks*. Singapore: Springer Nature Singapore, 2022, pp. 1395–1405.

[10] R. Li, B. Liu, C. Lu, H. Duan, and J. Shao, "A Worldwide View on the Reachability of Encrypted DNS Services," in *Web Conference 2024*, 2024.

[11] P. E. Hoffman and P. McManus, "DNS queries over HTTPS (doh)," *RFC*, vol. 8484, pp. 1–21, 2018. [Online]. Available: https://doi.org/10.17487/RFC8484

[12] Z. Hu, L. Zhu, J. S. Heidemann, A. Mankin, D. Wessels, and P. E. Hoffman, "Specification for DNS over transport layer security (TLS)," *RFC*, vol. 7858, pp. 1–19, 2016. [Online]. Available: https://doi.org/10.17487/RFC7858

[13] C. Huitema, S. Dickinson, and A. Mankin, "DNS over dedicated QUIC connections," *RFC*, vol. 9250, pp. 1–27, 2022. [Online]. Available: https://doi.org/10.17487/RFC9250

[14] A. W. Christopher Wood, "Announcing experimental ddr in 1.1.1.1," https://blog.cloudflare.com/announcing-ddr-support/, March 2022.

[15] T. Pauly, E. Kinnear, C. A. Wood, P. McManus, and T. Jensen, "Discovery of designated resolvers," *RFC*, vol. 9462, pp. 1–16, 2023. [Online]. Available: https://doi.org/10.17487/RFC9462

[16] B. Schwartz, ""RFC 9461 Service Binding Mapping for DNS Servers"," https://www.ietf.org/rfc/rfc9461.html, November 2023.

[17] E. Rescorla, K. Oku, N. Sullivan, and C. A. Wood, "TLS Encrypted Client Hello," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-esni-24, Mar. 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-esni/24/

[18] B. Liu, C. Lu, H. Duan, Y. Liu, Z. Li, S. Hao, and M. Yang, "Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path," in *USENIX Security*, Aug. 2018.

[19] X. Li, C. Lu, B. Liu, Q. Zhang, Z. Li, H. Duan, and Q. Li, "The Maginot Line: Attacking the Boundary of DNS Caching Protection," in *USENIX Security*, Aug. 2023.

[20] A. Hilton, C. Deccio, and J. Davis, "Fourteen Years in the Life: A Root Server's Perspective on DNS Resolver Security," in *USENIX Security*, Aug. 2023.

[21] C. T. Deccio and J. Davis, "DNS privacy in practice and preparation," in *CoNEXT 2019*. USA: ACM, 2019, pp. 138–143.

[22] R. Li, X. Jia, Z. Zhang, J. Shao, R. Lu, J. Lin, X. Jia, and G. Wei, "A Longitudinal and Comprehensive Measurement of DNS Strict Privacy," *IEEE/ACM Transactions on Networking*, vol. 31, no. 6, 2023.

[23] T. Fiebig, S. F. Gürses, C. Gañán, E. Kotkamp, F. Kuipers, M. Lindorfer, M. Prisse, and T. Sari, "Heads in the Clouds? Measuring Universities' Migration to Public Clouds: Implications for Privacy & Academic Freedom," *Proc. Priv. Enhancing Technol.*, vol. 2023, no. 2, 2023.

[24] C. Lu, B. Liu, Z. Li, S. Hao, H. Duan, M. Zhang, C. Leng, Y. Liu, Z. Zhang, and J. Wu, "An end-to-end, large-scale measurement of DNS-over-encryption: How far have we come?" in *IMC*, 10 2019.

[25] L. Jin, S. Hao, H. Wang, and C. Cotton, "Understanding the impact of encrypted DNS on internet censorship," in *WWW 2021*, 4 2021.

[26] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, "Comparing the Effects of DNS, DoT, and DoH on Web Performance," in *WWW 2020*, 4 2020.

[27] J. Zirngibl, P. Sattler, and G. Carle, "A first look at SVCB and HTTPS DNS resource records in the wild," in *IEEE European Symposium on Security and Privacy, EuroS&P 2023 - Workshops, Delft, Netherlands, July 3-7, 2023*. IEEE, 2023, pp. 470–474. [Online]. Available: https://doi.org/10.1109/EuroSPW59978.2023.00058

[28] Z. Durumeric, E. Wustrow, and J. A. Halderman, "Zmap: Fast internet-wide scanning and its security applications," in *USENIX Security*, 2013.

[29] M. Kührer, T. Hupperich, J. Bushart, C. Rossow, and T. Holz, "Going wild: Large-scale classification of open DNS resolvers," in *IMC*, 2015.

[30] O. Gasser, Q. Scheitle, P. Foremski, Q. Lone, M. Korczynski, S. D. Strowes, L. Hendriks, and G. Carle, "Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists," in *IMC*, 2018.

[31] J. Zirngibl, L. Steger, P. Sattler, O. Gasser, and G. Carle, "Rusty Clusters? Dusting an IPv6 Research Foundation," in *IMC*, 2022.

[32] L. Steger, L. Kuang, J. Zirngibl, G. Carle, and O. Gasser, "Target Acquired? Evaluating Target Generation Algorithms for IPv6," in *TMA*, 2023.

[33] J. Dickinson, S. Dickinson, R. Bellis, A. Mankin, and D. Wessels, "DNS Transport over TCP - Implementation Requirements," RFC 7766, Mar. 2016. [Online]. Available: https://www.rfc-editor.org/info/rfc7766

[34] MaxMind, "Geolite2 free geolocation data," 2024. [Online]. Available: https://dev.maxmind.com/geoip/geolite2-free-geolocation-data

[35] PeeringDB, ""PeeringDB"," https://www.peeringdb.com, 2004.

[36] S. Sassalla, "DoE-Hunter," Apr. 2025. [Online]. Available: https://doi.org/10.5281/zenodo.15276648

[37] ——, "Dataset - A First Look on Discovery of Designated Resolvers," Apr. 2025. [Online]. Available: https://doi.org/10.5281/zenodo.15275839

[38] T. V. Doan, J. Fries, and V. Bajpai, "Evaluating public dns services in the wake of increasing centralization of dns," in *IFIP Networking*, 2021.

[39] M. Kosek, L. Schumann, R. Marx, T. V. Doan, and V. Bajpai, "DNS privacy with speed?: evaluating DNS over QUIC and its impact on web performance," in *IMC*, 2022.

[40] B. Schwartz, M. Bishop, and E. Nygren, "Service binding and parameter specification via the DNS (SVCB and HTTPS resource records)," *RFC*, vol. 9460, pp. 1–47, 2023. [Online]. Available: https://doi.org/10.17487/RFC9460

[41] D. F. F. Boeira, E. J. Scheid, M. F. Franco, L. Zembruzki, and L. Z. Granville, "Traffic Centralization and Digital Sovereignty: An Analysis Under the Lens of DNS Servers," in *NOMS 2024*, May 2024, pp. 1–9.

[42] C. Xu, Y. Zhang, F. Shi, H. Shan, B. Guo, Y. Li, and P. Xue, "Measuring the Centrality of DNS Infrastructure in the Wild," *Applied Sciences*, '23.

[43] T. Shreedhar, R. Panda, S. Podanev, and V. Bajpai, "Evaluating QUIC Performance Over Web, Cloud Storage, and Video Workloads," *IEEE Transactions on Network and Service Management*, 2022.

[44] P. E. Hoffman, A. Sullivan, and K. Fujiwara, "DNS Terminology," RFC 7719, Dec. 2015.

[45] E. Kinnear, P. McManus, T. Pauly, T. Verma, and C. A. Wood, "Oblivious DNS over HTTPS," *RFC*, vol. 9230, pp. 1–19, 2022. [Online]. Available: https://doi.org/10.17487/RFC9230

[46] T. Pauly and T. Reddy.K, "Discovery of Oblivious Services via Service Binding Records," RFC 9540, Feb. 2024.

[47] S. Singanamalla, S. Chunhapanya, J. Hoyland, M. Vavruša, T. Verma, P. Wu, M. Fayed, K. Heimerl, N. Sullivan, and C. Wood, "Oblivious DNS over HTTPS (ODoH): A Practical Privacy Enhancement to DNS," *PoPET*, vol. 2021, no. 4, p. 575–592, Jul. 2021.