# Evaluating the Impact of Legacy DNS Vulnerabilities in FutureG Mobile Networks

Sana Habib
Arizona State University, Tempe, AZ, United States
Washington and Lee University, Lexington, VA, United States
shabib3@asu.edu / shabib@wlu.edu

***Abstract*—Unlike traditional IP and IP-based SDN networks, DNS in 5G and emerging 6G networks functions as a control-plane dependency, supporting telephony service discovery, SIP/IMS signaling (e.g., ENUM E.164 number mapping as a DNS application), and cross-slice traffic steering. Despite cloud-native, virtualized, and sliced architectures, DNS continues to rely on largely unchanged protocols and operational practices, leaving legacy vulnerabilities exposed. In this paper, we systematically analyze 84 documented DNS threats through an architecture-aware framework that evaluates their impact across six dimensions: service disruption, privacy leakage, amplification risk, traffic steering, slice impact, and misconfiguration risk. Our analysis highlights mobile-specific factors—including shared core functions, cross-slice resolvers, and DNS-mediated telephony control—that amplify the effects of protocol downgrades, incomplete DNSSEC deployment, and resolver sharing. In combination, these factors allow localized DNS failures to propagate across services, privacy boundaries, traffic steering, and slice isolation. We present a taxonomy that captures how DNS vulnerabilities manifest in next-generation mobile networks and map a subset of representative high-impact threats to architectural enforcement points, providing guidance for measurement, mitigation, and more robust 5G/6G design.**

## I. Introduction

Imagine a critical 5G or emerging 6G service failing because a minor DNS misconfiguration disrupts telephony service discovery, halts mobility signaling, or exposes subscriber traffic. Real-world incidents illustrate the plausibility of such cascading failures. In October 2025, a DNS-related failure in AWS's US-EAST-1 region propagated across hundreds of cloud services, affecting platforms from Snapchat to Reddit [1]. Similarly, a nationwide AT&T outage in February 2024 was traced to a misconfigured network element that triggered an automated shutdown of wireless services [2].

While these events did not originate exclusively from mobile DNS infrastructure, they underscore how configuration errors and control-plane dependencies can propagate rapidly in highly automated, distributed systems [3]–[10]. DNS in mobile networks differs in important ways from its role in traditional IP and IP-based Software-Defined Networking (SDN) environments (details in Appx. A) [11]. Beyond hostname resolution, DNS underpins telephony service discovery, SIP/IMS[1] signaling (e.g., ENUM [15]), network function discovery, and cross-slice service routing. As 5G deployments scale and 6G designs emerge, cloud-native, software-defined, and edge-integrated architectures increase the coupling between DNS and core control-plane functions. However, DNS protocols and many operational practices remain largely unchanged, leaving legacy weaknesses exposed and, in some cases, amplified [16].

In mobile networks, DNS functions as a shared control-plane dependency rather than a peripheral infrastructure service. DNS resolution directly influences network function discovery, mobility workflows, telephony control, and inter-service communication within service-based cores [16]. Consequently, DNS failures or attacks can cascade across network slices, disrupt telephony session establishment, and leak subscriber identifiers or service metadata. Longstanding weaknesses—such as resolver misconfigurations, incomplete DNSSEC deployment, and outdated software—persist, while mobile-specific architectural features including shared resolvers, cross-slice dependencies, and DNS-mediated telephony control (ENUM/IMS) can magnify their operational impact [15], [18]–[21].

We consider 5G and 6G together as future-generation (*FutureG*) mobile networks because both rely on service-based architectures, virtualized network functions, and DNS-mediated service discovery. As a result, DNS risks observed in 5G are likely to persist—and potentially intensify—as networks evolve toward 6G. This dependency is particularly relevant as FutureG networks support ultra-reliable low-latency communications, massive machine-type communications, and large-scale IoT deployments, where control-plane disruptions can propagate across tightly coupled services and administrative domains [22]–[25].

In this work, we systematically analyze 84 documented DNS threats in 5G and emerging 6G networks using an architecture-aware framework. We examine how legacy DNS weaknesses interact with mobile-specific architectural features, which security properties they affect, and how their consequences are shaped by sliced, cloud-native cores. We make three primary contributions:

[1]SIP (Session Initiation Protocol) [12] controls multimedia session setup, while IMS (IP Multimedia Subsystem) [13], [14] delivers SIP-based voice, video, and messaging in 3G–6G networks.

Workshop on Security and Privacy of Next-Generation Networks (FutureG) 2026
23 February 2026, San Diego, CA, USA
ISBN 979-8-9919276-9-7
https://dx.doi.org/10.14722/futureg.2026.23093
www.ndss-symposium.org

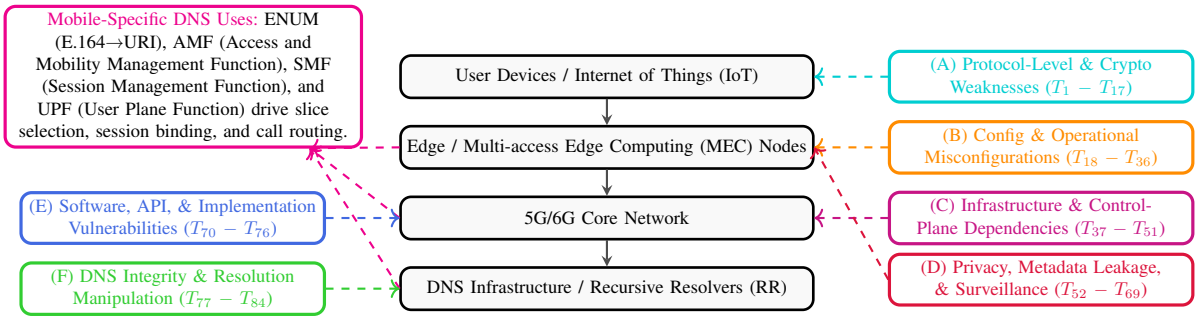


**Fig. 1:** Layered DNS dependencies in the FutureG mobile networks stack—from user/IoT devices to edge/MEC, 5G/6G core, and recursive resolvers—illustrate six threat categories (A–F, Sec. V) and show how mobile DNS functions (E.164 Number Mapping (ENUM) [15], Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF)) drive slice selection, session binding, call routing, and allow failures to propagate beyond application reachability, potentially disrupting telephony signaling and cross-slice service delivery [17].

- We develop a systematic taxonomy of DNS threats tailored to next-generation mobile architectures.
- We show that legacy DNS weaknesses remain relevant even in highly virtualized, multi-tenant, and logically isolated network deployments.
- We identify architectural and deployment factors that can amplify DNS-related risk and map representative high-impact threats to architectural enforcement points, providing guidance for improving the resilience of FutureG networks.

## II. Why DNS Threats?

DNS is a foundational control-plane dependency in 5G and emerging 6G networks. Unlike traditional IP or SDN environments [11], where DNS primarily resolves hostnames for end hosts, mobile networks rely on DNS for telephony service discovery, control-plane signaling, and service-based core operations. Misconfigurations or protocol flaws can propagate across layers, slices, and services, turning minor errors into systemic risks that disrupt mobility signaling, slice isolation, or inter-service communication.

### A. Why DNS Threats Matter

In cloud-native mobile cores, DNS integrates tightly with service-based architectures, virtualized network functions, network slicing, and edge deployments. Beyond basic name resolution, it supports network function discovery, slice bootstrap, and telephony signaling (e.g., ENUM-based IMS resolution). Legacy flaws or misconfigurations can cascade across slices, disrupt telephony services, misdirect traffic, or leak subscriber information [16], [22], [23]. Mobile networks differ fundamentally from enterprise or SDN deployments: DNS resolution directly affects mobility management, session establishment, and inter-function communication, and shared core components can amplify failures across tenants, creating systemic control-plane risks largely absent in traditional networks.

### B. Related DNS Taxonomies and Threat Assessments

Prior DNS taxonomies and measurements focus on protocol flaws, resolver behavior, and operational misconfigurations in traditional Internet settings [18], [26]–[29], assuming static trust boundaries and limited service coupling. Security surveys for 5G/6G often treat DNS as peripheral, emphasizing authentication, RAN, and core protocols [16], [30]–[33]. Our work bridges these perspectives by analyzing 84 documented DNS threats in FutureG networks, demonstrating how mobile-specific dependencies amplify legacy weaknesses and create systemic control-plane risks that demand architecture-aware mitigation and secure design.

## III. DNS Threats in FutureG Networks

DNS is a critical control-plane dependency in 5G and emerging 6G networks, enabling telephony service discovery, slice orchestration, and traffic routing from user devices to edge, core, and resolver infrastructure (Fig. 1). Misconfigurations or protocol flaws can propagate across layers, slices, and services, potentially causing service disruption.[2]

At the *user device and IoT layer*, DNS supports telephony discovery, authentication, and early mobility signaling; failures can impair connectivity and latency-sensitive applications [34]. At the *edge/MEC layer*, DNS directs queries to edge instances and slices; misconfigurations may compromise slice isolation, expose telemetry, or reduce performance [35]–[37]. At the *5G/6G core*, DNS maintains service-to-slice mappings, mobility management, and inter-slice coordination; failures can cascade, disrupting multiple services and tenants [38], [39]. At the *DNS infrastructure and recursive resolver layer*, attacks or misconfigurations—e.g., cache poisoning or spoofing—can propagate upward, undermining correctness, availability, and reliability [40].

While FutureG inherits standard DNS threats from IP and IP-based SDN networks, mobile-specific features—shared resolvers, cross-slice dependencies, and DNS-mediated telephony control (ENUM/IMS)—amplify their impact [15], [41]. These factors make DNS a high-leverage failure point, motivating layer-specific mitigation and enforcement strategies discussed later.

[2]In this paper, we use the terms service disruption and telephony service disruption interchangeably.

**TABLE I:** Adversarial Taxonomy for DNS threats in FutureG Mobile Networks.

| *ID* | *Adversary Type* | *Primary Capabilities* | *Targeted DNS Components* | *Typical Attack Mechanisms* |
|---|---|---|---|---|
| $A_1$ | On-Path Attackers | Intercept or manipulate DNS traffic at access, edge, or transit links, affecting mobility, slice routing, & telephony services. | Client–resolver paths; recursive caches. | Query/response injection; tampering; passive monitoring. |
| $A_2$ | Off-Path Attackers | Exploit protocol or deployment weaknesses remotely, impacting resolution integrity or service availability. | Exposed resolvers; edge caches. | Cache poisoning; protocol downgrade; reflection/amplification. |
| $A_3$ | Compromised Resolvers | Control recursive resolution logic in multi-tenant or cross-slice deployments. | Recursive resolvers; caches; shared infrastructure. | Response injection; selective censorship; metadata exfiltration; telephony service disruption. |
| $A_4$ | Malicious Domain Owners / Registrars | Manipulate authoritative domain names and delegations, affecting routing and service discovery. | Authoritative zones; delegation records. | Domain hijacking; malicious records; traffic steering. |
| $A_5$ | Insiders / Misconfiguration-Capable Operators | Misconfigure or abuse privileged access in orchestration/management planes. | Resolvers; orchestration planes; slice management. | Misconfiguration; policy abuse; DNSSEC disablement; telephony disruption. |
| $A_6$ | Cross-Tenant Attackers | Exploit shared infrastructure in multi-tenant or sliced deployments, impacting co-resident services. | Shared resolvers; edge platforms; slice-adjacent services. | Side-channel leakage; cross-slice interference; shared-state abuse; telephony service disruption. |

## IV. Adversarial Taxonomy and Behaviors

DNS vulnerabilities in next-generation mobile networks extend beyond classical on-path attackers. Cloud-native architectures—including network slicing, edge computing, and multi-tenant deployments—expand both the adversary set and attack surface [42]–[47]. Because DNS is shared across slices and virtualized functions, a single weakness can be exploited by external attackers, insiders, compromised infrastructure, or co-resident tenants, blurring traditional trust boundaries and enabling attacks to propagate across services.

To reason systematically, we introduce an adversarial taxonomy classifying attackers by capability and architectural leverage, linking them to DNS assets, attack mechanisms, and potential systemic impact ($A_1$–$A_6$). Table I summarizes the taxonomy.

### A. Adversary Classes

We identify six classes based on access and architectural leverage: On-path ($A_1$) and Off-path ($A_2$) attackers represent classical network threats, capable of intercepting or manipulating DNS traffic, with impact amplified by mobility, telephony service discovery, and slice-specific routing. Compromised resolvers ($A_3$) and Malicious domain owners or registrars ($A_4$) capture infrastructure-level threats, enabling response manipulation, traffic steering, or metadata exfiltration. Insiders or misconfiguration-capable operators ($A_5$) represent operational risks where human error or privilege abuse can have systemic consequences. Cross-tenant attackers ($A_6$) exploit shared infrastructure in virtualized or sliced deployments, affecting co-resident tenants without direct network access. These six classes cover external, internal, infrastructural, and architectural adversaries without overlap.[3]

### B. Adversary Capabilities

Adversaries differ in access, visibility, and technical sophistication. $A_1$ attackers intercept or manipulate traffic at access or edge networks [48]. $A_2$ attackers exploit protocol weaknesses remotely, including cache poisoning [49] and downgrade attacks [50]. $A_3$ attackers compromise resolvers to inject responses, selectively censor, exfiltrate metadata, or disrupt telephony services [46]. $A_4$ attackers operate at the domain or registrar level, enabling hijacking or abuse of traffic steering [51]. $A_5$ attackers introduce misconfiguration or privileged misuse in orchestration and management planes [30], [47], [52]. $A_6$ attackers exploit shared infrastructure in multi-tenant or sliced deployments, affecting co-resident services and slices [53].

### C. Adversarial Behaviors

We characterize behaviors along three dimensions, linking them to attacker classes, DNS threats ($T_1$–$T_{84}$), and six evaluation dimensions (Sec. VI-B).

*1) Targeted Components:* Resolver-level attacks—such as cache poisoning or amplification—primarily involve $A_1$, $A_2$, and $A_3$. Attacks on authoritative zones or DNS management infrastructure involve $A_4$ and $A_5$. Client- and edge-facing attacks additionally engage $A_6$ in shared or sliced networks.

*2) Attack Goals:* Adversaries target availability, integrity, and confidentiality. Telephony service disruption involves $A_1$, $A_2$, $A_3$, $A_5$, and $A_6$. Traffic redirection and integrity violations involve $A_1$–$A_5$, while metadata collection and privacy compromise involve $A_1$, $A_3$, and $A_6$.

*3) Attack Mechanisms:* Misconfigurations are exploited by $A_3$–$A_6$; incomplete DNSSEC deployment by $A_2$ and $A_3$; exposed or open resolvers by $A_2$ and $A_3$; and passive DNS observation by $A_1$, $A_3$, and $A_6$.

This taxonomy systematically links adversary classes, behaviors, and mechanisms to DNS threats, providing a structured framework for understanding persistent DNS risks in FutureG networks and guiding layer-specific mitigation and enforcement strategies.

## V. Threat Taxonomy

Building on the layered architecture in Fig. 1, we synthesized a corpus of roughly eighty DNS threats across six cat-

[3]Additional justification for the six adversary classes is provided in Appx. C.

egories, derived from academic research, operational reports, and publicly disclosed incidents.

*Corpus Construction Methodology*

We systematically collected sources using keyword searches, reference mining, and CVE analysis of DNS software and infrastructure. The corpus draws from: (i) academic studies of DNS vulnerabilities in legacy and modern networks (CCS, CCSW, IEEE S&P, NDSS, PETS, USENIX Security); (ii) 5G/6G architectural specifications; and (iii) documented operational misconfigurations. From these, we selected 84 high-impact threats for detailed analysis.

Each threat is analyzed by mechanism, affected network layer, and potential impact on telephony service continuity, privacy, and security. Threats are mapped to one or more of the six categories in Fig. 1, forming Tables V, VI, and VII (Appx. B). Our methodology organizes existing DNS risks within the realities of FutureG architectures rather than introducing new attacks.

### A. Protocol-Level and Cryptographic Weaknesses ($T_1$–$T_{17}$)

This category encompasses mobile-specific protocol and cryptographic weaknesses. For example, misconfigured DNSSEC in ENUM domains ($T_{17}$, Table V, Appx. B) can enable spoofed responses that misroute IP Multimedia Subsystem (IMS) sessions [13], [14] and calls, directly affecting telephony service discovery in 5G/6G networks [54].

### B. Configuration & Operational Misconfigurations ($T_{18}-T_{36}$)

These threats arise from human or operational errors and are increasingly critical in automated 5G/6G networks. For example, mistakes in ENUM zone delegation or record management ($T_{32}$, Table V, Appx. B) can misroute E.164-based service discovery, disrupting IMS call setup and session management. Moreover, such misconfigurations can propagate across slices, shared resolvers, and edge deployments, amplifying telephony service disruption and cross-tenant effects [54].

### C. Infrastructure and Control-Plane Dependencies ($T_{37}-T_{51}$)

These threats stem from coupling between DNS and core control-plane functions. DNS underpins service orchestration, slice management, and mobility workflows; failures can cascade across slices and network functions. ENUM-based E.164 resolution failures, for instance, can disrupt control-plane service discovery and IMS session setup [54] ($T_{51}$, Table VI, Appx. B).

### D. Privacy, Metadata Leakage, and Surveillance ($T_{52}-T_{69}$)

Threats in this category expose DNS metadata or query patterns without directly affecting availability or integrity. For example, ENUM queries for IMS services can reveal user session details or service usage to passive observers in 5G/6G networks [54] ($T_{69}$, Table VI, Appx. B). Edge and multi-tenant deployments further increase the granularity of observable metadata by reducing traffic aggregation and introducing slice- or tenant-specific resolution contexts, making query patterns more easily attributable to individual users, services, or network slices.

### E. Software, API, & Impl. Vulnerabilities ($T_{70}-T_{76}$)

This category captures flaws in resolver software, management APIs, and orchestration systems. For example, weak input validation or authentication in 5G SBA/NEF/CAPIF[4] APIs ($T_{76}$ in Table VII, Appx. B) exposes DNS service discovery endpoints to spoofing or injection, potentially degrading resolution or telephony service binding [41], [55], [58]. These vulnerabilities can disrupt traffic steering, cache correctness, or service availability in multi-slice, cloud-native deployments.

### F. DNS Integrity and Resolution Manipulation ($T_{77}-T_{84}$)

These threats involve deliberate manipulation of DNS resolution, targeting correctness rather than software or configuration. For example, $T_{84}$ (*Resolver Failover Manipulation* in Table VII, Appx. B) [59] interferes with failover mechanisms, redirecting queries to malicious servers or inducing service disruption. Such attacks can bypass slice isolation and affect multi-tenant deployments, amplifying impact on telephony and cross-slice service delivery in FutureG networks.

## VI. Evaluation Methodology

We evaluate each DNS threat in next-generation mobile networks under realistic 5G/6G deployment assumptions, systematically quantifying its potential impact on security, privacy, and operations. Our methodology accounts for both traditional risks and mobile-specific factors—such as network slicing, edge deployments, and service-based architectures—providing a comprehensive, architecture-aware assessment of 84 persistent threats[5].

### A. Evaluation Approach

Each threat is assessed along six complementary dimensions capturing security, privacy, reliability, and operational risks: telephony service disruption, privacy leakage, amplification risk, traffic steering, impact on network slices, and misconfiguration risk.

For each dimension, we assign a qualitative severity rating—*high* (●), *medium* (◆), or *low* (■)—reflecting potential impact in realistic deployments. Ratings are based on: (i) prior literature and documented incidents, (ii) the threat's underlying mechanism, and (iii) architecture-aware reasoning rather than exploit prevalence alone. A *high* (●) rating indicates substantial impact even with mitigations, whereas a *low* (■) rating indicates localized effects unlikely to propagate beyond a single function, slice, or service.

### B. Evaluation Dimensions

Threats are evaluated across six dimensions, each capturing a distinct consequence of DNS vulnerabilities:

[4]In 5G Service-Based Architectures (SBA) [17], [55], core network functions expose services via standardized interfaces. The Network Exposure Function (NEF) [17], [55] securely publishes capabilities to authorized consumers, while the Common API Framework (CAPIF) [56], [57] provides a unified framework for secure API discovery, authentication, and authorization across 5G networks.

[5]Deployment assumptions, including network slicing, service-based interfaces, and edge computing, are detailed in Appx. D.

*1) Service Disruption:* Potential to impair telephony availability or reliability, including IMS session setup, call signaling, voice or messaging services, and service-based interfaces. Failures can propagate across slices and services, amplified by interconnected control-plane orchestration, service discovery, and dependency on DNS resolution [30], [38].

*2) Privacy Leakage:* Potential to expose sensitive information about subscribers, services, or network operations. Adversaries may infer DNS query metadata, service identifiers, or slice-specific communication patterns. Even encrypted DNS can leak metadata if query minimization or padding is not properly applied [44], [45], [60].

*3) Amplification Risk:* Potential for a threat to magnify traffic volumes or exploit DNS infrastructure to induce large-scale denial-of-service effects, affecting internal or external resources and creating systemic risks [42], [43].

*4) Traffic Steering:* Potential to manipulate DNS resolution outcomes, including cache poisoning, domain hijacking, or exploitation of DNS-based load balancing and traffic steering, which may bypass slice isolation, disrupt routing policies, or undermine subscriber trust [51], [59].

*5) Impact on Network Slices:* Potential to compromise slice or tenant isolation. Attacks may propagate through shared control-plane components, causing cross-slice interference, information leakage, or service disruption in multi-tenant deployments [61], [62].

*6) Misconfiguration Risk:* Likelihood that operational complexity or human error introduces persistent vulnerabilities. Examples include incomplete DNSSEC deployment, stale or inconsistent records, or fragile dependency chains. In automated, cloud-native networks, misconfigurations can be systemic, affecting multiple slices, functions, and telephony services simultaneously [30], [42], [63].

## VII. Evaluation Insights

We evaluate 84 DNS threats (Tables V–VII, Appx. B) under realistic 5G/6G deployment assumptions using the six evaluation dimensions defined in Sec. VI-B. Each threat is assessed according to its technical mechanism, operational context, and potential impact on telephony service continuity, privacy, and network integrity.

Recurring patterns emerge across threat categories. Threats rarely remain localized: failures in one layer—such as fallback negotiation, cache state, or resolver configuration—can cascade into IMS session disruption, traffic steering, and slice interference. Multi-tenant deployments amplify these effects, as shared resolvers and tightly coupled control-plane functions turn minor weaknesses (e.g., incomplete DNSSEC enforcement or delayed updates) into high-impact or high misconfiguration-risk events. Individual threats often span multiple adversary capabilities ($A_2$, $A_3$, $A_5$), highlighting the importance of architecture-aware, rather than threat-specific, risk assessment.

To illustrate, we discuss representative threats from each category: A in Sec. VII-A and B–F in Appx. E–I to save space. The complete evaluation, mapping threat types to impact dimensions and adversary capabilities, is summarized in Tables II and III.

### A. Protocol-Level and Cryptographic Weaknesses

Category A captures fundamental protocol and cryptographic weaknesses that persist in next-generation mobile networks. A representative example is *ENUM DNSSEC Integrity Failure* ($T_{17}$) [54], where misconfigured ENUM DNSSEC allows attackers to inject spoofed DNS responses, misrouting SIP/IMS sessions and disrupting telephony services.

Under realistic 5G/6G assumptions (provided in Appx. D), the threat is rated as follows (see Table II, row $T_{17}$): *telephony service disruption* is *high* (●), since spoofed ENUM responses can prevent SIP registrations, block call setups, or redirect signaling; *privacy leakage* is *high* (●), as attackers can observe user identifiers, IMS subscription information, and slice-specific metadata; *amplification risk* is *medium* (◆), because a single compromised ENUM resolver can propagate forged entries across multiple subscribers; *traffic steering* is *medium* (◆), due to potential misdirection of SIP signaling paths between slices or tenants; *impact on network slices* is *high* (●), as shared ENUM infrastructure links multiple slices; and *misconfiguration risk* is *high* (●), reflecting the operational complexity of maintaining correct DNSSEC keys and signatures in distributed ENUM deployments.

This threat is exploitable by off-path attackers ($A_2$), who can inject spoofed responses without direct access to user traffic, and by malicious or compromised resolvers ($A_3$), which can propagate integrity failures across slices. It demonstrates how protocol-level DNSSEC weaknesses cascade through control-plane components, disrupting SIP/IMS services and threatening operational security and telephony privacy in 5G/6G networks.

### B. Cross-Category Observations on DNS Threats

Analyzing all six threat categories (A–F) in 5G/6G deployments reveals clear trends across each evaluation dimension.

*1) Service Disruption:* Infrastructure- and implementation-focused threats (A, B, C, E) frequently cause high disruption (●), whereas privacy-centric attacks (Category D) rarely affect telephony services.

*2) Privacy Leakage:* Category D threats consistently have high privacy impact (●), e.g., excessive DNS logging ($T_{52}$) and DNS query fingerprinting ($T_{54}$). Some rebinding attacks (Category F) also leak metadata, indicating that observation often accompanies active attacks.

*3) Amplification Risk:* Amplification potential is generally low (■), with only select routing or API attacks able to leverage misconfigurations for broader effect.

*4) Traffic Steering:* Certain attacks, including DNS hijacking ($T_{57}$), Anycast abuse ($T_{59}$), and resolver failover manipulation ($T_{84}$), can reroute signaling or traffic, affecting specific network slices without causing complete telephony outages.

**TABLE II:** Evaluation of persistent DNS threats under realistic 5G/6G deployment assumptions (Categories A, B, C). *Keys:* High (●), Medium (◆), Low (■), and colored labels indicate exploitable adversary classes ($A_1$–$A_6$).

| ID | DNS Threat | Service Disrup. | Privacy Leakage | Amp. Risk | Traffic Steering | Impact on Network Slices | Misconfig. Risk | Exploitable Adversary Types |
|---|---|---|---|---|---|---|---|---|
| A: Protocol-Level and Cryptographic Weaknesses (Sec. V-A) | | | | | | | | |
| $T_1$ | DNS-over-TLS Certificate Misvalidation [48] | ● | ● | ◆ | ◆ | ◆ | ■ | $A_1$, $A_2$ |
| $T_2$ | DNS Cache Poisoning [49] | ● | ◆ | ◆ | ◆ | ● | ◆ | $A_2$, $A_3$ |
| $T_3$ | Plaintext DNS Exposure [64] | ◆ | ● | ■ | ◆ | ● | ■ | $A_1$ |
| $T_4$ | Incomplete DNSSEC Deployment [19] | ● | ◆ | ◆ | ◆ | ● | ● | $A_2$, $A_3$ |
| $T_5$ | DNSSEC Misconfiguration [65] | ● | ◆ | ◆ | ◆ | ● | ● | $A_2$, $A_3$ |
| $T_6$ | NXDOMAIN Hijacking [66] | ◆ | ◆ | ■ | ◆ | ◆ | ◆ | $A_1$, $A_2$ |
| $T_7$ | DNS Tunneling [67], [68] | ◆ | ● | ◆ | ◆ | ◆ | ◆ | $A_2$, $A_3$, $A_4$ |
| $T_8$ | Long TTL Abuse [69] | ◆ | ■ | ■ | ◆ | ◆ | ◆ | $A_3$, $A_5$ |
| $T_9$ | Resolver Capability Downgrade Attacks [50] | ● | ◆ | ◆ | ◆ | ◆ | ● | $A_2$, $A_3$ |
| $T_{10}$ | DNSSEC Key Exhaustion [70] | ● | ■ | ◆ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{11}$ | Algorithm Downgrade Attacks [50] | ● | ■ | ◆ | ◆ | ◆ | ◆ | $A_2$, $A_3$ |
| $T_{12}$ | Fragmentation-Based DNS Attacks [71] | ◆ | ◆ | ◆ | ◆ | ◆ | ■ | $A_1$, $A_2$ |
| $T_{13}$ | EDNS0 Abuse [18] | ◆ | ■ | ◆ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{14}$ | Protocol-Level DNS Downgrade Attacks [50] | ● | ◆ | ◆ | ◆ | ● | ● | $A_2$, $A_3$ |
| $T_{15}$ | Stale DNSSEC Key Retention [46] | ◆ | ◆ | ◆ | ◆ | ◆ | ● | $A_3$, $A_5$ |
| $T_{16}$ | DNSSEC Algorithm Downgrade [50] | ● | ◆ | ◆ | ◆ | ● | ● | $A_2$, $A_3$ |
| $T_{17}$ | *ENUM DNSSEC Integrity Failure* [54] | ● | ● | ◆ | ◆ | ● | ● | $A_2$, $A_3$ |
| B: Configuration and Operational Misconfigurations (Sec. V-B) | | | | | | | | |
| $T_{18}$ | Misconfigured Wildcard Records [72], [73] | ◆ | ◆ | ■ | ◆ | ◆ | ● | $A_5$, $A_6$ |
| $T_{19}$ | Operational DNS Debt [42] | ◆ | ◆ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{20}$ | Insecure Bootstrap Resolvers [74] | ● | ◆ | ◆ | ◆ | ◆ | ● | $A_2$, $A_3$ |
| $T_{21}$ | Misconfigured Reverse DNS (PTR) [75] | ◆ | ■ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{22}$ | Registrar Account Takeover [76] | ● | ● | ◆ | ◆ | ● | ● | $A_4$, $A_5$ |
| $T_{23}$ | DNS Policy Inconsistency [77] | ◆ | ◆ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{24}$ | Stale DNS Records [78] | ◆ | ● | ■ | ◆ | ● | ● | $A_5$ |
| $T_{25}$ | Lame Delegations [79] | ◆ | ◆ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{26}$ | Missing Response Rate Limiting (RRL) [43] | ◆ | ■ | ● | ◆ | ◆ | ● | $A_5$ |
| $T_{27}$ | Edge DNS Misconfiguration [63] | ◆ | ◆ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{28}$ | Split-Horizon DNS Errors [80] | ◆ | ◆ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{29}$ | Lack of DNS Redundancy [52] | ● | ■ | ◆ | ◆ | ◆ | ● | $A_5$ |
| $T_{30}$ | Misconfigured Forwarders [81] | ◆ | ■ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{31}$ | Incorrect Glue Records [78] | ◆ | ■ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{32}$ | *IMS ENUM Zone Misconfiguration* [54] | ● | ◆ | ■ | ◆ | ● | ● | $A_3$, $A_5$ |
| $T_{33}$ | Broken Fallback Resolvers [82] | ◆ | ■ | ■ | ◆ | ◆ | ● | $A_3$, $A_5$ |
| $T_{34}$ | IPv6 DNS Misalignment [83], [84] | ◆ | ■ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{35}$ | Operational Visibility Gaps [85] | ◆ | ◆ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{36}$ | Recursive Resolver Looping [86], [87] | ◆ | ◆ | ◆ | ◆ | ◆ | ● | $A_3$, $A_5$ |
| C: Infrastructure and Control-Plane Dependencies (Sec. V-C) | | | | | | | | |
| $T_{37}$ | Cross-Slice DNS Leakage [61] | ◆ | ● | ■ | ◆ | ● | ● | $A_3$, $A_6$ |
| $T_{38}$ | Control-Plane DNS Dependence [88] | ● | ◆ | ◆ | ◆ | ● | ◆ | $A_3$ |
| $T_{39}$ | Weak Access Controls on DNS APIs [89] | ● | ● | ◆ | ◆ | ● | ● | $A_3$, $A_5$ |
| $T_{40}$ | DNS-based Service Discovery Failures [47], [90] | ◆ | ◆ | ◆ | ◆ | ◆ | ● | $A_5$ |
| $T_{41}$ | NF Resolution Poisoning [47] | ● | ◆ | ◆ | ◆ | ● | ● | $A_3$, $A_5$ |
| $T_{42}$ | Slice Bootstrap DNS Failures [30] | ● | ◆ | ◆ | ◆ | ● | ● | $A_3$, $A_5$ |
| $T_{43}$ | Open Recursive Resolvers [91] | ◆ | ◆ | ● | ● | ◆ | ● | $A_2$, $A_3$ |
| $T_{44}$ | Dependency on Third-Party DNS [92] | ◆ | ● | ■ | ◆ | ● | ● | $A_3$, $A_4$ |
| $T_{45}$ | DNS-based Traffic Steering Abuse [62] | ◆ | ◆ | ■ | ◆ | ◆ | ◆ | $A_3$, $A_4$ |
| $T_{46}$ | Resolver Trust Assumptions [88] | ◆ | ◆ | ◆ | ◆ | ◆ | ● | $A_3$ |
| $T_{47}$ | Core Network DNS Flooding [93] | ● | ■ | ● | ◆ | ● | ◆ | $A_1$, $A_2$ |
| $T_{48}$ | Misaligned DNS Load Balancing [94] | ◆ | ◆ | ■ | ◆ | ◆ | ● | $A_5$ |
| $T_{49}$ | Cross-Tenant Resolver Contamination [53] | ◆ | ● | ■ | ◆ | ● | ● | $A_3$, $A_6$ |
| $T_{50}$ | DNS Dependency Loops [95] | ● | ◆ | ◆ | ◆ | ● | ● | $A_3$, $A_5$ |
| $T_{51}$ | *Resolution Failures in 3GPP Control Plane* [54] | ● | ◆ | ■ | ◆ | ● | ● | $A_3$, $A_5$ |

*5) Impact on Network Slices:* Multi-dimensional threats—especially software and API vulnerabilities (Category E)—can degrade slice performance. Infrastructure attacks (Categories A, B, C, F) also target slices selectively, highlighting localized adversary impact.

*6) Misconfiguration Risk:* Weak APIs, memory bugs, and mismanaged updates increase misconfiguration exposure, enabling both passive and active attackers to exploit infrastructure more easily.

Finally, passive observers ($A_1$) dominate privacy threats, active manipulators ($A_2$, $A_3$) target routing and software, and specialized adversaries ($A_4$–$A_6$) appear in API or slice-specific attacks, reflecting diverse attacker capabilities. Overall, DNS threats in modern networks are multi-faceted: some

**TABLE III:** Evaluation of persistent DNS threats under realistic 5G/6G deployment assumptions (Categories D, E, F). *Keys:* High (●), Medium (◆), Low (■, and colored labels indicate exploitable adversary classes ($A_1$–$A_6$).

| ID | DNS Threat | Service Disrup. | Privacy Leakage | Amp. Risk | Traffic Steer-ing | Impact on Network Slices | Misconfig. Risk | Exploitable Adversary Types |
|---|---|---|---|---|---|---|---|---|
| D: Privacy, Metadata Leakage, and Surveillance (Sec. V-D) | | | | | | | | |
| $T_{52}$ | Excessive DNS Logging [96] | ■ | ● | ■ | ◆ | ◆ | ◆ | $A_1$, $A_3$ |
| $T_{53}$ | WebRTC DNS and IP Leakage [97] | ■ | ● | ■ | ◆ | ◆ | ◆ | $A_1$ |
| $T_{54}$ | DNS Query Fingerprinting [60], [98] | ■ | ● | ■ | ◆ | ◆ | ◆ | $A_1$ |
| $T_{55}$ | Encrypted SNI Correlation [99] | ■ | ● | ■ | ◆ | ◆ | ◆ | $A_1$ |
| $T_{56}$ | Resolver-side Profiling [100] | ■ | ● | ■ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{57}$ | DNS Hijacking [101], [102] | ● | ● | ◆ | ● | ● | ● | $A_2$, $A_3$ |
| $T_{58}$ | Anycast Manipulation [103] | ◆ | ◆ | ◆ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{59}$ | Anycast Routing Abuse [51] | ● | ◆ | ◆ | ◆ | ● | ◆ | $A_3$, $A_4$ |
| $T_{60}$ | GeoDNS Abuse [104] | ◆ | ◆ | ■ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{61}$ | ISP-level NXDOMAIN Rewriting [105] | ◆ | ● | ■ | ◆ | ◆ | ◆ | $A_1$ |
| $T_{62}$ | DNS Enumeration [106] | ■ | ◆ | ■ | ◆ | ◆ | ◆ | A1, $A_3$ |
| $T_{63}$ | DNS over HTTPS Policy Bypass [107] | ◆ | ◆ | ■ | ◆ | ◆ | ◆ | $A_1$ |
| $T_{64}$ | Encrypted DNS Traffic Analysis [44], [45] | ■ | ◆ | ■ | ◆ | ◆ | ◆ | $A_1$ |
| $T_{65}$ | DNS-based Service Enumeration [108], [109] | ■ | ◆ | ■ | ◆ | ◆ | ◆ | $A_1$, $A_3$ |
| $T_{66}$ | Resolver Cache Snooping [96], [110] | ■ | ◆ | ■ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{67}$ | DNS-based Covert Signaling [111], [112] | ◆ | ◆ | ◆ | ◆ | ◆ | ◆ | $A_1$, $A_2$ |
| $T_{68}$ | DNS Logging Jurisdictional Risk [113], [114] | ◆ | ◆ | ◆ | ◆ | ◆ | ◆ | $A_1$ |
| $T_{69}$ | *IMS Service Metadata Exposure via DNS* [54] | ◆ | ● | ◆ | ◆ | ◆ | ◆ | $A_1$ |
| E: Software, API, and Implementation Vulnerabilities (Sec. V-E) | | | | | | | | |
| $T_{70}$ | Insecure Dynamic DNS Updates [115] | ● | ◆ | ■ | ◆ | ● | ● | $A_2$, $A_3$ |
| $T_{71}$ | Resolver Software Vulnerabilities [116] | ● | ◆ | ◆ | ◆ | ● | ◆ | $A_2$, $A_3$ |
| $T_{72}$ | Memory Corruption Bugs [117] | ● | ● | ◆ | ◆ | ● | ◆ | $A_2$, $A_3$ |
| $T_{73}$ | API Token Reuse [89] | ◆ | ● | ■ | ◆ | ● | ◆ | $A_2$, $A_3$ |
| $T_{74}$ | Orchestrator–DNS Desynchronization [118] | ◆ | ◆ | ■ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{75}$ | Resolver Fingerprinting [119] | ■ | ◆ | ■ | ◆ | ◆ | ◆ | $A_1$, $A_3$ |
| $T_{76}$ | *Weak 5G Core DNS API Hardening* [41], [58] | ● | ◆ | ■ | ◆ | ● | ● | $A_3$, $A_5$ |
| F: DNS Integrity and Resolution Manipulation (Sec. V-F) | | | | | | | | |
| $T_{77}$ | DNS Rebinding Attacks [120], [121] | ◆ | ● | ■ | ◆ | ◆ | ◆ | $A_1$, $A_4$ |
| $T_{78}$ | Resolution-State Manipulation [122] | ◆ | ◆ | ■ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{79}$ | Negative Caching Abuse [123] | ◆ | ■ | ■ | ◆ | ◆ | ◆ | $A_3$, $A_5$ |
| $T_{80}$ | TTL Manipulation Attacks [18], [124] | ◆ | ■ | ■ | ◆ | ◆ | ◆ | $A_3$, $A_5$ |
| $T_{81}$ | Malicious DNS Prefetching [125] | ◆ | ◆ | ◆ | ◆ | ◆ | ◆ | $A_3$ |
| $T_{82}$ | DNS-based Phishing Infrastructure [126] | ◆ | ● | ■ | ● | ◆ | ● | $A_2$, $A_3$ |
| $T_{83}$ | DNS Shadowing [127] | ◆ | ● | ■ | ◆ | ◆ | ● | $A_2$, $A_3$ |
| $T_{84}$ | *Resolver Failover Manipulation* [59] | ◆ | ◆ | ■ | ● | ● | ◆ | $A_1$, $A_3$, $A_5$ |

cause overt telephony/service disruption, while others enable subtle information leakage or targeted manipulation, underlining the need for evaluation across all six dimensions.

Taken together, these cross-category observations show that DNS in 5G/6G networks is not a single-point failure domain, but a layered control-plane dependency whose security, reliability, and privacy implications must be assessed across threat categories, attacker capabilities, and architectural layers.

### C. Strategies for Mitigating DNS Threats in 5G/6G

DNS threats span multiple layers, so no single mitigation strategy can address all vulnerabilities. We analyze a subset of representative threats to illustrate how to apply mitigations and where to enforce controls across the layered DNS architecture, including the user/IoT layer, edge/MEC layer, 5G/6G core, and recursive resolver layer, while considering trade-offs such as operational complexity. Table IV summarizes the proposed strategies. For brevity, we focus on representative threat from Category A; mitigation strategies for representative threats from Categories B–F appear in Appx. E-I.

For *ENUM DNSSEC Integrity Failure* ($T_{17}$) [54], integrity failures arise from permissive DNSSEC deployment and fallback behavior in ENUM resolution. Such threats can be *mitigated* by (see Table IV, row $T_{17}$) enforcing mandatory DNSSEC validation at ENUM resolvers, explicitly disabling insecure fallback paths, and managing trust anchors across operators. These controls should be enforced primarily at the core signaling infrastructure (e.g., ENUM resolvers supporting IMS and interconnect services) to prevent telephony-wide misrouting, while edge-level validation can help limit local impact. The main trade-offs involve increased operational complexity due to strict DNSSEC enforcement, including key generation, secure rotation, trust anchor management, and cross-operator coordination. There is also higher key management overhead, as resolvers must maintain and regularly update cryptographic keys and trust anchors, and potential interoperability challenges with legacy operators who may not fully support DNSSEC.

This example illustrates that effective mitigation in 5G/6G DNS systems requires enforcing controls at the appropriate layer—core or edge—while balancing operational complexity,

**TABLE IV:** Representative Mapping of High-Impact DNS Threats to Controls and Enforcement Points in 5G/6G Mobile Networks (Telephony-Focused).

| # | *Capability* | *Impact* | *Controls* | *Enforcement* | *Trade-Offs* |
|---|---|---|---|---|---|
| $T_{17}$ | ENUM DNSSEC Integrity Failure [54] | Telephony disruption: SIP/IMS registrations, call setup, and signaling across slices. | Validate DNSSEC. Disable insecure fallback paths. Manage trust anchors. | 5G/6G Core | Increased operational complexity. Key management overhead. Potential interoperability issues. |
| $T_{32}$ | IMS ENUM Zone Misconfiguration [54] | Telephony service failures: misrouted calls, incomplete IMS session setup, and exposure of subscriber info. | Automate zone validation. Configure with dependency awareness. Isolate slices at resolver level. (Appx. E) | 5G/6G Core, Edge/MEC | Operational overhead. Continuous monitoring. Inter-operator coordination required. (Appx. E) |
| $T_{51}$ | Resolution Failures in 3GPP Control Plane [54] | Telephony disruptions due to ENUM or control-plane resolution failures affecting IMS call/session setup. | Orchestrate with dependency awareness. Add resolver redundancy. Synchronize state. Deploy anomaly detection. (Appx. F) | 5G/6G Core, Edge/MEC | Orchestration complexity. Monitoring requirements. Cross-service coordination required. (Appx. F) |
| $T_{69}$ | IMS Service Metadata Exposure via DNS [54] | Telephony metadata leakage: IMS session info and subscriber identifiers inferred from DNS queries. | Minimize records. Use split-horizon or private resolvers. Enforce access control. Apply rate limiting. (Appx. G) | 5G/6G Core, Edge/MEC | Operational overhead. Added latency. Inter-slice coordination required. (Appx. G) |
| $T_{76}$ | Weak 5G Core DNS APIs [41], [58] | Telephony disruption via API abuse impacting IMS or ENUM resolution. | Enforce authentication and authorization. Validate inputs. Apply rate limiting. Conduct security audits (Appx. H). | 5G/6G Core | Operational overhead. Additional latency. Cross-slice coordination required (Appx. H). |
| $T_{84}$ | Resolver Failover Manipulation [59] | Telephony signaling disruptions: manipulated resolver failover misroutes calls or blocks IMS sessions. | Tune failover. Validate fallback behavior. Monitor resolver activity. (Appx. I) | Edge/MEC, DNS Infrastructure/RR | Operational overhead. Added latency. Monitoring complexity (Appx. I). |

monitoring requirements, and inter-operator coordination. The remaining representative threats and their mitigation strategies appear in Appx. E-I.

## VIII. Discussion

This work synthesizes persistent DNS threats in 5G and emerging 6G networks using a layered architectural perspective and a capability-driven adversary taxonomy. Rather than advocating a single defense, our goal is to highlight where DNS remains a fragile dependency and how next-generation architectures can amplify long-standing risks. Minor protocol weaknesses or operational misconfigurations can cascade through IMS signaling, slice orchestration, and resolver infrastructure, causing telephony disruptions, traffic steering, and cross-slice interference.

### A. Forward-Looking Recommendations and Validation

In 6G architectures, DNS should be treated as an explicit control-plane component. Practical measures include limiting legacy fallback mechanisms, aligning slice-specific trust boundaries with resolver placement, and combining automation with resolver validation and isolation. Embedding runtime monitoring and automated configuration checks can further reduce the likelihood and impact of cascading failures.

Empirical validation of the presented threat taxonomy could be pursued in 5G or early 6G testbeds, such as Open5GS [128] or OpenAirInterface [129], [130]. Experiments could, for example, introduce resolver misconfigurations to observe cross-slice propagation, measure latency and availability under traffic amplification or downgrade attacks, and evaluate metadata exposure through DNS-based inference. Such studies would help quantify operational trade-offs and guide future deployment strategies.

### B. Limitations

Our study has three main limitations. First, the taxonomy relies on public literature and documented incidents; proprietary practices are not represented. Second, the assessment is qualitative, focusing on relative impact rather than probability. Third, threat prevalence is not measured; the analysis characterizes feasible failure modes rather than their frequency. Vendor-specific implementations are abstracted, and evolving 6G designs may alter threat manifestations. Despite these limitations, our findings highlight persistent DNS dependencies and provide a foundation for targeted mitigations and empirical validation.

## IX. Conclusion

DNS is a critical control-plane dependency in 5G and emerging 6G networks, where minor misconfigurations or legacy behaviors can cascade across multi-tenant, sliced architectures. Our analysis of 84 documented threats using an architecture-aware taxonomy highlights persistent high-leverage weaknesses, including incomplete DNSSEC, protocol downgrades, resolver sharing, and operational misconfigurations. Securing DNS in next-generation mobile networks is inherently socio-technical: protocol design, software engineering, operational discipline, and inter-operator coordination jointly determine risk. By mapping a small subset of representative threats to concrete mitigations, this work provides actionable guidance for designers and operators to treat DNS as a first-class control-plane component.

## Acknowledgements

This work was supported by the Fulbright Fellowship, the HIVE Fellowship at the Center for Digital Resilience, and the

Graduate Fellowship Award from Arizona State University. The views, opinions, findings, and conclusions expressed in this material are solely those of the author and do not necessarily reflect those of the Fulbright Program, the HIVE Fellowship, Arizona State University, or their affiliated institutions. The author thanks Durdana Habib for the initial inspiration for this work and gratefully acknowledges the Fall 2025 Computer Networks class at W&L—particularly Micah Tongen, Brandon Bishop, Nick Lagges, Trey Custodio, and Vincent Ziccardi—for their intellectual engagement and discussions that helped shape this research. The author also thanks the anonymous reviewers of FutureG'26 for their thoughtful and constructive feedback.

## REFERENCES

[1] TechRadar Pro, "Downtime caused historic issues in 2025 — but who lost out most?" *TechRadar*, 2025, https://www.techradar.com/pro/security/downtime-caused-historic-issues-in-2025-but-who-lost-out-most. [Online]. Available: https://www.techradar.com/pro/security/downtime-caused-historic-issues-in-2025-but-who-lost-out-most

[2] F. C. Commission, "FCC Report on AT&T Nationwide Wireless Outage," FCC Public Safety and Homeland Security Bureau, Tech. Rep., 2024, https://docs.fcc.gov/public/attachments/DOC-404150A1.pdf. [Online]. Available: https://docs.fcc.gov/public/attachments/DOC-404150A1.pdf

[3] (2025) Louisiana Probes Lapse After Agencies Suffer Online Outage. https://www.govtech.com/security/louisiana-probes-lapse-after-agencies-suffer-online-outage.

[4] (2025) Internet Outages Timeline. https://www.thousandeyes.com/resources/internet-outages-timeline.

[5] (2025) 2025's biggest internet outages and what caused them. https://betanews.com/2025/12/18/2025s-biggest-internet-outages-and-what-caused-them/.

[6] (2025) Yesterday's global internet outage caused by single file on Cloudflare servers — unexpected file size caused catastrophic error, knocking out several major websites. https://www.tomshardware.com/tech-industry/big-tech/yesterdays-global-internet-outage-caused-by-single-file-on-cloudflare-servers-unexpected-file-size-caused-catastrophic-error-knocking-out-several-major-websites.

[7] (2025) 2025 Global Network Outage report and Internet Health Check. https://www.networkworld.com/article/3630303/2025-global-network-outage-report-and-internet-health-check.html.

[8] (2025) Whisper Security Reveals 95.3% of Global Internet Vulnerable to DNS Hijacking. https://www.kron4.com/business/press-releases/ein-presswire/875608724/whisper-security-reveals-95-3-of-global-internet-vulnerable-to-dns-hijacking/.

[9] (2025) Google Finds Server Takeovers Linked to React2Shell Exploitation. https://www.esecurityplanet.com/threats/google-finds-server-takeovers-linked-to-react2shell-exploitation/.

[10] (2025) EdgeStepper Implant Reroutes DNS Queries to Deploy Malware via Hijacked Software Updates. https://thehackernews.com/2025/11/edgestepper-implant-reroutes-dns.html.

[11] S. Habib, J. R. Crandall, and A. Doupé, "Revisiting SDN Resilience in Cloud and Enterprise Environments," in *Proceedings of the 2025 Cloud Computing Security Workshop*, 2025, pp. 28–49.

[12] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session initiation protocol," RFC 3261, 2002.

[13] 3GPP, "IP Multimedia Subsystem (IMS); Stage 2," 3rd Generation Partnership Project, Tech. Rep. TS 23.228, 2023. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123400_123499/123406/07.01.00_60/ts_123406v070100p.pdf

[14] M. Poikselkä and G. Mayer, *The IMS: IP multimedia concepts and services*. John Wiley & Sons, 2013.

[15] N. vs Networking. Telco Network Engineering. (2021) ENUM – DNS based Call Routing. https://nickvsnetworking.com/enum-dns-based-call-routing/.

[16] M. Yang, Y. Qu, T. Ranbaduge, C. Thapa, N. H. Sultan, M. Ding, H. Suzuki, W. Ni, S. Abuadbba, D. Smith *et al.*, "From 5G to 6G: A survey on security, privacy, and standardization pathways," *ACM Computing Surveys*, 2024.

[17] 3GPP, "System Architecture for the 5G System (5GS)," 3rd Generation Partnership Project, Tech. Rep. TS 23.501, 2020, defines the Service-Based Architecture (SBA) and core network functions including NEF. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf

[18] T. H. Kim and D. Reeves, "A survey of Domain Name System Vulnerabilities and Attacks," *Journal of Surveillance, Security and Safety*, vol. 1, pp. 34–60, 2020.

[19] T. Chung, R. van Rijswijk-Deij, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson, "A Longitudinal, End-to-End View of the DNSSEC Ecosystem," in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1307–1322.

[20] DN.org. (2025) DNSSEC Adoption Rates, Barriers, and Progress in Securing the Domain Name System. [Online]. Available: https://dn.org/dnssec-adoption-rates-barriers-and-progress-in-securing-the-domain-name-system

[21] "DNSSEC Validation Rate by Country." https://stats.labs.apnic.net/dnssec.

[22] M. E. Haque, F. Tariq, M. R. Khandaker, M. S. Hossain, M. A. Imran, and K.-K. Wong, "A Comprehensive Survey of 5G URLLC and Challenges in the 6G Era," *arXiv preprint arXiv:2508.20205*, 2025.

[23] J. Miao, Z. Wang, M. Wang, X. Feng, N. Xiao, and X. Sun, "Security authentication protocol for massive machine type communication in 5G networks," *Wireless Communications and Mobile Computing*, vol. 2023, no. 1, p. 6086686, 2023.

[24] M. Muhammad and G. A. Safdar, "5G-based V2V broadcast communications: A security perspective," *Array*, vol. 11, p. 100084, 2021.

[25] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, "Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation," *Transportation Research Part C: Emerging Technologies*, vol. 68, pp. 168–184, 2016.

[26] A. Ramdas and R. Muthukrishnan, "A survey on DNS security issues and mitigation techniques," in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*. IEEE, 2019, pp. 781–784.

[27] G. Schmid, "Thirty years of DNS insecurity: Current issues and perspectives," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2429–2459, 2021.

[28] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A survey on DNS encryption: Current development, malware misuse, and inference techniques," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–28, 2022.

[29] N. Usman Aijaz, M. Misbahuddin, and S. Raziuddin, "Survey on DNS-specific security issues and solution approaches," in *Data Science and Security: Proceedings of IDSCS 2020*. Springer, 2020, pp. 79–89.

[30] J. Dias, P. Pinto, R. Santos, and S. Malta, "5G network slicing: Security challenges, attack vectors, and mitigation approaches," *Sensors*, vol. 25, no. 13, p. 3940, 2025.

[31] P. Scalise, M. Boeding, M. Hempel, H. Sharif, J. Delloiacovo, and J. Reed, "A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas," *Future Internet*, vol. 16, no. 3, p. 67, 2024.

[32] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," *Computer Networks*, vol. 221, p. 109515, 2023.

[33] R. Barker and F. Afghah, "Securing Open RAN: A Survey of Cryptographic Challenges and Emerging Solutions for 5G," *arXiv preprint arXiv:2506.09418*, 2025.

[34] DNS.org Staff, "DNS in Mobile Networks and 5G Architecture: Enabling Next Generation Connectivity and Service Resolution," https://dn.org/dns-in-mobile-networks-and-5g-architecture-enabling-next-generation-connectivity-and-service-resolution/, 2025.

[35] "DNS in 5G and Edge Computing: Reducing Latency at the Network Edge," https://dn.org/dns-in-5g-and-edge-computing-reducing-latency-at-the-network-edge/, DNS.org Staff, 2024.

[36] "Revolutionizing Connectivity with Edge DNS in 5G Networks," https://dn.org/revolutionizing-connectivity-with-edge-dns-in-5g-networks/, DNS.org Staff, 2024.

[37] R. Harrilal-Parchment, D. Pineda, K. Akkaya, A. Aydeger, and A. Perez-Pons, "Bringing DNS service to 5G Edge for Reduced Latencies in mMTC Applications," in *2023 IEEE International Conference on Information Technology (ICIT)*, 2023.

[38] DNS.org Staff, "DNS in Mobile Networks and 5G Architecture: Enabling Next Generation Connectivity and Service Resolution," https://dn.org/dns-in-mobile-networks-and-5g-architecture-enabling-next-generation-connectivity-and-service-resolution/, 2025.

[39] "DNS in 5G Core Networks: Innovations for Low Latency Services," https://dn.org/dns-in-5g-core-networks-innovations-for-low-latency-services/, DNS.org Staff, 2025.

[40] DNS.org Staff, "DNS Cache Poisoning Attacks: Past, Present and Future," https://dn.org/dns-cache-poisoning-historical-attacks-and-modern-defenses/, 2025.

[41] PixelsSEO, "5G Network API Security: 2026 Technical Guide," https://pixelsseo.com/5g-network-api-security/, 2026.

[42] V. Pappas, Z. Xu, S. Lu, D. Massey, A. Terzis, and L. Zhang, "Impact of configuration errors on DNS robustness," in *Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, 2004, pp. 319–330.

[43] C. Deccio, D. Argueta, and J. Demke, "A quantitative study of the deployment of DNS rate limiting," in *2019 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2019, pp. 442–447.

[44] S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, and C. Troncoso, "Encrypted DNS $\rightarrow$ privacy? A traffic analysis perspective," *arXiv preprint arXiv:1906.09682*, 2019.

[45] J. Bushart and C. Rossow, "Padding Ain't Enough: Assessing the privacy guarantees of encrypted DNS," in *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.

[46] E. Osterweil, P. F. Tehrani, T. C. Schmidt, and M. Wählisch, "From the beginning: Key transitions in the first 15 years of DNSSEC," *IEEE transactions on network and service management*, vol. 19, no. 4, pp. 5265–5283, 2022.

[47] (2010) DNS-Based Service Discovery (DNS-SD) Privacy and Security Requirements. RFC 8882. https://datatracker.ietf.org/doc/rfc8882/.

[48] T. V. Doan, I. Tsareva, and V. Bajpai, "Measuring DNS over TLS from the edge: Adoption, reliability, and response times," in *International Conference on Passive and Active Network Measurement*. Springer, 2021, pp. 192–209.

[49] N. Alexiou, S. Basagiannis, P. Katsaros, T. Dashpande, and S. A. Smolka, "Formal analysis of the kaminsky DNS cache-poisoning attack using probabilistic model checking," in *2010 IEEE 12th International Symposium on High Assurance Systems Engineering*. IEEE, 2010, pp. 94–103.

[50] E. Heftrig, H. Shulman, and M. Waidner, "Downgrading DNSSEC: How to Exploit Crypto Agility for Hijacking Signed Zones," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 7429–7444.

[51] X. Fan, J. Heidemann, and R. Govindan, "Evaluating anycast in the domain name system," in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 1681–1689.

[52] C. Deccio, J. Sedayao, K. Kant, and P. Mohapatra, "Measuring availability in the domain name system," in *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, pp. 1–5.

[53] G. Moav, Y. Afek, A. Bremler-Barr, and A. Klein, "DNS FLaRE: A Flush-Reload attack on DNS Forwarders," in *34th USENIX Security Symposium (USENIX Security 25)*, 2025, pp. 3557–3576.

[54] P. Faltstrom and M. Mealling, "RFC3761: The E. 164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)," 2004.

[55] 3GPP, "Procedures for the 5G System (5GS)," 3rd Generation Partnership Project, Tech. Rep. TS 23.502, 2024. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145

[56] 3GPP, "3GPP CAPIF Framework - RNAA," 3rd Generation Partnership Project, Tech. Rep., 2023. [Online]. Available: https://www.3gpp.org/technologies/rnaa

[57] ETSI / 3GPP, "Security aspects of the Common API Framework (CAPIF)," ETSI / 3rd Generation Partnership Project, Tech. Rep. TS 33.122, 2024, describes security architecture and mechanisms for CAPIF in 5G SBA. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133100_133199/133122/18.03.00_60/ts_133122v180300p.pdf

[58] A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru, "Cross-Service Token: Finding Attacks in 5G Core Networks," *arXiv preprint arXiv:2509.08992*, 2025. [Online]. Available: https://arxiv.org/abs/2509.08992

[59] Q. Zhang, X. Bai, X. Li, H. Duan, Q. Li, and Z. Li, "{ResolverFuzz}: Automated discovery of {DNS} resolver vulnerabilities with {Query-Response} fuzzing," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 4729–4746.

[60] D. W. Kim and J. Zhang, "You are how you query: Deriving behavioral fingerprints from DNS traffic," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2015, pp. 348–366.

[61] B. Imana, A. Korolova, and J. Heidemann, "Enumerating Privacy Leaks in DNS Data Collected above the Recursive," in *NDSS: DNS Privacy Workshop*, 2018.

[62] E. Tsai, D. Kumar, R. S. Raman, G. Li, Y. Eiger, and R. Ensafi, "CERTainty: Detecting DNS manipulation at Scale using TLS certificates," *arXiv preprint arXiv:2305.08189*, 2023.

[63] Y. Wang, K. Yu, Z. Wang, K. Hu, H. Du, Q. Xiang, X. Fang, G. Li, R. Zhou, L. Kong *et al.*, "Rethinking DNS Configuration Verification with a Distributed Architecture," in *Proceedings of the 8th Asia-Pacific Workshop on Networking*, 2024, pp. 23–30.

[64] S. Siby, M. Juarez, N. Vallina-Rodriguez, C. Troncoso *et al.*, "DNS Privacy not so private: the traffic analysis perspective," in *The 11th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2018)*, 2018.

[65] N. L. van Adrichem, N. Blenn, A. R. Lúa, X. Wang, M. Wasif, F. Fatturrahman, and F. A. Kuipers, "A measurement study of DNSSEC misconfigurations," *Security Informatics*, vol. 4, no. 1, p. 8, 2015.

[66] G. Liu, L. Jin, S. Hao, Y. Zhang, D. Liu, A. Stavrou, and H. Wang, "Dial "N" for NSDomain: The Scale, Origin, and Security Implications of DNS Queries to Non-Existent Domains," in *Proceedings of the 2023 ACM on Internet Measurement Conference*, 2023, pp. 198–212.

[67] D. Tatang, F. Quinkert, N. Dolecki, and T. Holz, "A study of newly observed hostnames and DNS tunneling in the wild," *arXiv preprint arXiv:1902.08454*, 2019.

[68] Y. Wang, A. Zhou, S. Liao, R. Zheng, R. Hu, and L. Zhang, "A comprehensive survey on DNS tunnel detection," *Computer Networks*, vol. 197, p. 108322, 2021.

[69] G. C. Moura, J. Heidemann, R. d. O. Schmidt, and W. Hardaker, "Cache me if you can: Effects of DNS time-to-live," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 101–115.

[70] E. Heftrig, H. Schulmann, N. Vogel, and M. Waidner, "The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024, pp. 497–510.

[71] A. Herzberg and H. Shulman, "Fragmentation considered poisonous, or: One-domain-to-rule-them-all. org," in *2013 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2013, pp. 224–232.

[72] D. Barr, "RFC1912: Common DNS Operational and Configuration Errors," 1996.

[73] A. Kalafut, M. Gupta, P. Rattadilok, and P. Patel, "Surveying DNS Wildcard Usage among the Good, the Bad, and the Ugly," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2010, pp. 448–465.

[74] A. Hilton, C. Deccio, and J. Davis, "Fourteen Years in the Life: A Root Server's Perspective on DNS Resolver Security," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 3171–3186.

[75] O. van der Toorn, R. van Rijswijk-Deij, R. Sommese, A. Sperotto, and M. Jonker, "Saving Brian's privacy: The perils of privacy exposure through reverse DNS," in *Proceedings of the 22nd ACM Internet Measurement Conference*, 2022, pp. 1–13.

[76] G. Akiwate, S. Savage, G. M. Voelker, and K. C. Claffy, "Risky BIZness: Risks Derived from Registrar Name Management," in *Proceedings of the 21st ACM Internet Measurement Conference*, 2021, pp. 673–686.

[77] R. Sommese, G. C. Moura, M. Jonker, R. van Rijswijk-Deij, A. Dainotti, K. C. Claffy, and A. Sperotto, "When parents and children disagree: Diving into DNS delegation inconsistency," in *International Conference on Passive and Active Network Measurement*. Springer, 2020, pp. 175–189.

[78] Y. Zhang, B. Liu, H. Duan, M. Zhang, X. Li, F. Shi, C. Xu, and E. Alowaisheq, "Rethinking the Security Threats of Stale DNS Glue

Records," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 1261–1277.

[79] (2009) Impact of configuration errors on DNS robustness. IBM. https://research.ibm.com/publications/impact-of-configuration-errors-on-dns-robustness.

[80] (2022) Split-Horizon DNS Configuration. https://www.ietf.org/archive/id/draft-reddy-add-enterprise-split-dns-06.html.

[81] X. Zheng, C. Lu, J. Peng, Q. Yang, D. Zhou, B. Liu, K. Man, S. Hao, H. Duan, and Z. Qian, "Poison over troubled forwarders: A cache poisoning attack targeting DNS forwarding devices," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 577–593.

[82] D. Yang, Z. Li, and G. Tyson, "A deep dive into DNS query failures," in *2020 USENIX Annual Technical Conference (USENIX ATC 20)*, 2020, pp. 507–514.

[83] F. Streibelt, P. Sattler, F. Lichtblau, C. H. Ganán, A. Feldmann, O. Gasser, and T. Fiebig, "How ready is DNS for an IPv6-only world?" in *International Conference on Passive and Active Network Measurement*. Springer, 2023, pp. 525–549.

[84] L. Hendriks, P.-T. de Boer, and A. Pras, "IPv6-specific misconfigurations in the DNS," in *2017 13th International Conference on Network and Service Management (CNSM)*. IEEE, 2017, pp. 1–5.

[85] M. Stevanovic, J. M. Pedersen, A. D'Alconzo, S. Ruehrup, and A. Berger, "On the ground truth problem of malicious DNS traffic analysis," *computers & security*, vol. 55, pp. 142–158, 2015.

[86] Y. Afek, A. Bremler-Barr, and L. Shafir, "NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 631–648. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/afek

[87] Y. Afek, A. Bremler-Barr, and S. Stajnrod, "NRDelegationAttack: Complexity DDoS attack on DNS recursive resolvers," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 3187–3204.

[88] V. Ramasubramanian and E. G. Sirer, "Perils of Transitive Trust in the Domain Name System," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, 2005, pp. 35–35.

[89] Z. Mousavi, C. Islam, M. A. Babar, A. Abuadbba, and K. Moore, "Detecting misuse of security APIs: A systematic review," *ACM Computing Surveys*, vol. 57, no. 12, pp. 1–39, 2025.

[90] C.-F. Liao and Y.-J. Weng, "Enabling Space-Aware Service Discovery Model in Home Networks through a Compatible Extension to mDNS/DNS-SD," *Electronics*, vol. 12, no. 18, p. 3885, 2023.

[91] J. Park, R. Jang, M. Mohaisen, and D. Mohaisen, "A large-scale behavioral analysis of the open DNS resolvers on the internet," *IEEE/ACM Transactions on Networking*, vol. 30, no. 1, pp. 76–89, 2021.

[92] S. Wang, K. MacMillan, B. Schaffner, N. Feamster, and M. Chetty, "Measuring the Consolidation of DNS and Web Hosting Providers," *arXiv preprint arXiv:2110.15345*, 2021.

[93] R. Sommese, K. Claffy, R. van Rijswijk-Deij, A. Chattopadhyay, A. Dainotti, A. Sperotto, and M. Jonker, "Investigating the impact of DDoS attacks on DNS infrastructure," in *proceedings of the 22nd ACM Internet Measurement Conference*, 2022, pp. 51–64.

[94] F. Zhang, B. Liu, E. Alowaisheq, J. Chen, C. Lu, L. Song, Y. Ma, Y. Liu, H. Duan, and M. Yang, "Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS servers," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 296–310.

[95] J. G. Kagwe and M. Masinde, "Survey on DNS configurations, interdependencies, resilience and security for*. ke domains," in *Proceedings of the 2nd ACM Symposium on Computing for Development*, 2012, pp. 1–1.

[96] IETF DNS PRIVate Exchange Working Group, "RFC 9076: DNS Privacy Considerations," https://datatracker.ietf.org/doc/rfc9076/, 2021.

[97] A. F. K. Koysha, A. Boyaci, and R. Akdeniz, "WebRTC Metadata and IP leakage in Modern Browsers: A Cross-Platform Measurement Study," *arXiv preprint arXiv:2510.16168*, 2025.

[98] O. Arana, H. Benítez-Pérez, J. Gomez, and M. Lopez-Guerrero, "Never Query Alone: A distributed strategy to protect internet users from DNS fingerprinting attacks," *Computer Networks*, vol. 199, p. 108445, 2021.

[99] Z. Chai, A. Ghafari, and A. Houmansadr, "On the importance of Encrypted-SNI (ESNI) to censorship circumvention," in *9th USENIX Workshop on Free and Open Communications on the Internet (FOCI 19)*, 2019.

[100] A. Jimenez-Berenguel, C. Gil, C. Garcia-Rubio, J. Forné, and C. Campo, "DNS Query Forgery: A Client-side Defense Against Mobile App Traffic Profiling," *IEEE Access*, 2025.

[101] G. Akiwate, R. Sommese, M. Jonker, Z. Durumeric, K. Claffy, G. M. Voelker, and S. Savage, "Retroactive identification of targeted DNS infrastructure hijacking," in *Proceedings of the 22nd ACM Internet Measurement Conference*, 2022, pp. 14–32.

[102] M. Fejrskov, J. M. Pedersen, and E. Vasilomanolakis, "Detecting DNS hijacking by using Netflow data," in *2022 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2022, pp. 273–280.

[103] A. Rizvi, L. Bertholdo, J. Ceron, and J. Heidemann, "Anycast agility: Network playbooks to fight DDoS," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 4201–4218.

[104] R. A. Fainchtein, A. J. Aviv, M. Sherr, S. Ribaudo, and A. Khullar, "Holes in the Geofence: Privacy Vulnerabilities in "Smart" DNS Services," *arXiv preprint arXiv:2012.07944*, 2020.

[105] P. Pearce, B. Jones, F. Li, R. Ensafi, N. Feamster, N. Weaver, and V. Paxson, "Global measurement of DNS manipulation," in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 307–323.

[106] A. Paul, H. Islam, S. Hossain, and H. S. Narman, "A Novel Zone-walking Protection for Secure DNS Server," *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)*, vol. 14, no. 1, pp. 1–15, 2022.

[107] J. Lee, D. Mohaisen, and M. S. Kang, "Measuring DNS-over-HTTPS Downgrades: Prevalence, Techniques, and Bypass Strategies," *Proceedings of the ACM on Networking*, vol. 2, no. CoNEXT4, pp. 1–22, 2024.

[108] F. B. Wala and S. Bohacek, "Zone-Hopping: Sensitive Information Leakage Prevention for DNSSEC-NSEC," in *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*. IEEE, 2024, pp. 104–110.

[109] S. Goldberg, M. Naor, D. Papadopoulos, L. Reyzin, S. Vasant, and A. Ziv, "NSEC5: Provably Preventing DNSSEC Zone Enumeration," *Cryptology ePrint Archive*, 2014.

[110] A. Randall, E. Liu, G. Akiwate, R. Padmanabhan, G. M. Voelker, S. Savage, and A. Schulman, "Trufflehunter: Cache Snooping Rare Domains at Large Public DNS Resolvers," in *Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 50–64.

[111] S. Saeli, F. Bisio, P. Lombardo, and D. Massa, "DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach," *arXiv preprint arXiv:2010.01582*, 2020.

[112] S. Chen, B. Lang, H. Liu, D. Li, and C. Gao, "DNS covert channel detection method using the LSTM model," *Computers & Security*, vol. 104, p. 102095, 2021.

[113] 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 2024-2024 IEEE Network Operations and Management Symposium*. IEEE, 2024, pp. 1–9.

[114] T. D. N. Encyclopedia. (2025) Legal Aspects of Cross Border DNS Data Sharing. https://dn.org/legal-aspects-of-cross-border-dns-data-sharing/.

[115] Y. Nosyk, M. Korczyński, C. H. Gañán, M. Król, Q. Lone, and A. Duda, "Don't Get Hijacked: Prevalence, Mitigation, and Impact of Non-Secure DNS Dynamic Updates," in *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2023, pp. 1480–1489.

[116] Q. Zhang, X. Bai, X. Li, H. Duan, Q. Li, and Z. Li, "ResolverFuzz: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 4729–4746.

[117] K. Man, Z. Qian, Z. Wang, X. Zheng, Y. Huang, and H. Duan, "DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 1337–1350.

[118] P. D. Bojović and S. Gajin, "An approach to evaluation of common DNS misconfigurations," *arXiv preprint arXiv:1711.05696*, 2017.

[119] D. W. Kim and J. Zhang, "Deriving and measuring DNS-based fingerprints," *Journal of Information Security and Applications*, vol. 36, pp. 32–42, 2017.

[120] C. Jackson, A. Barth, A. Bortz, W. Shao, and D. Boneh, "Protecting browsers from DNS rebinding attacks," *ACM Transactions on the Web (TWEB)*, vol. 3, no. 1, pp. 1–26, 2009.

[121] M. Hazhirpasand, A. A. Ebrahim, and O. Nierstrasz, "Stopping DNS Rebinding Attacks in the Browser." in *ICISSP*, 2021, pp. 596–603.
[122] M. Lyu, H. H. Gharakheili, C. Russell, and V. Sivaraman, "Analyzing Enterprise DNS Traffic to Classify Assets and Track Cyber-Health," *arXiv preprint arXiv:2201.07352*, 2022.
[123] D. Eastlake 3rd, C. Kaufman, S. Crocker, "Negative Caching of DNS Queries (DNS NCACHE)," RFC 2308, Internet Engineering Task Force (IETF), 1998, https://www.rfc-editor.org/rfc/rfc2308.html.
[124] T. Hernandez-Quintanilla, E. Magaña, D. Morató, and M. Izal, "On the reduction of authoritative DNS cache timeouts: Detection and implications for user privacy," *Journal of Network and Computer Applications*, vol. 176, p. 102941, 2021.
[125] S. Krishnan and F. Monrose, "DNS prefetching and its privacy implications: when good things go bad," in *Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*, 2010, pp. 10–10.
[126] T. Koide, N. Fukushi, H. Nakano, and D. Chiba, "PhishReplicant: A language model-based approach to detect generated squatting domain names," in *Proceedings of the 39th Annual Computer Security Applications Conference*, 2023, pp. 1–13.
[127] MITRE ATT&CK, "T1584.001: Domain Shadowing," https://attack.mitre.org/techniques/T1584/001/, 2024.
[128] Open5GS Community, "Open5GS: Open Source 5G Core and EPC," https://github.com/open5gs/open5gs, 2025.
[129] F. Kaltenberger, A. P. Silva, A. Gosain, L. Wang, and T.-T. Nguyen, "OpenAirInterface: Democratizing innovation in the 5G Era," *Computer Networks*, vol. 176, p. 107284, 2020.
[130] Q. Douarre, E.-M. Djelloul, P. Berthou, D. Dragomirescu, and P. Owezarski, "Design of a 5G experimental platform based on OpenAirInterface," in *International Conference on Testbeds and Research Infrastructures*. Springer, 2022, pp. 87–103.
[131] S. Habib, T. Bao, Y. Shoshitaishvili, and A. Doupé, "Mitigating threats emerging from the interaction between SDN apps and SDN (configuration) datastore," in *Proceedings of the 2022 on Cloud Computing Security Workshop*, 2022, pp. 23–39.
[132] P. Faltstrom and R. Danley, "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database," Internet Engineering Task Force (IETF), RFC 3403, October 2002. [Online]. Available: https://datatracker.ietf.org/doc/rfc3403/
[133] P. Faltstrom and E. Nygren, "The Naming Authority Pointer (NAPTR) DNS Resource Record," Internet Engineering Task Force (IETF), RFC 2915, September 2000. [Online]. Available: https://datatracker.ietf.org/doc/rfc2915/

## APPENDIX

### A. Why DNS Has Distinct Security Implications in Mobile Networks?

Mobile networks adopt software-defined and cloud-native architectures similar to those used in IP-based SDN environments, but DNS plays a fundamentally different role. In 5G and emerging 6G systems, DNS resolution directly supports service discovery, traffic steering, and slice-specific policy enforcement. Because these mechanisms depend on DNS outcomes before higher-level controls act, failures or misconfigurations can propagate across slices and subscribers, influencing telephony signaling and network behavior in ways that differ from traditional SDN control-plane failures [11], [131].

*1) DNS Precedes Policy and Traffic Steering:* In conventional SDN deployments, DNS primarily serves applications, and failures typically affect reachability or performance. In mobile networks, DNS can influence control-plane decisions that affect telephony signaling and session establishment; stale records, fallback behavior, or protocol downgrades may lead to incorrect policy application or misrouted signaling traffic. While such effects are not inevitable, DNS failures can propagate before policy enforcement or traffic steering occurs, giving DNS a distinct and earlier influence on telephony service continuity.

*2) Cross-Slice and Cross-Tenant Exposure:* Unlike SDN deployments that are often scoped to individual tenants or applications, mobile DNS infrastructure is frequently shared across slices, tenants, and services. As a result, misconfigurations or failures affecting telephony-related resolution in one slice may indirectly influence others. This shared dependency does not imply unavoidable cascading disruption, but it reduces isolation and increases the potential scope of telephony service impact.

*3) Failure Semantics and Observability:* DNS failures in mobile networks commonly manifest as latency increases, timeouts, or stale records. These symptoms can disrupt telephony signaling and session establishment while remaining transient and partially observable, complicating attribution and diagnosis. In contrast, SDN failures are typically more explicit and localized. The ambiguous nature of DNS failures underscores the need for careful monitoring when assessing telephony service disruptions.

*4) Legacy Protocol Assumptions in Virtualized Cores:* Despite highly virtualized and multi-tenant cores, mobile networks retain legacy DNS behaviors, including partial DNSSEC deployment, fallback mechanisms, and cache inconsistencies. These behaviors interact with cloud-native orchestration and shared infrastructure supporting telephony control. Unlike SDN frameworks explicitly designed for isolation and control-plane visibility, DNS remains a legacy dependency embedded in mobile telephony workflows, increasing shared risk in some scenarios without implying guaranteed failure.

*5) Implications for Future-Generation Mobile Networks:* DNS occupies a distinct position in 5G and 6G architectures: it informs telephony signaling behavior prior to traffic steering and policy enforcement, may propagate telephony service disruptions across slices under certain conditions, and is difficult to attribute using external observation alone. These characteristics motivate an architecture-aware analysis of DNS threats focused on telephony service resilience in future-generation mobile networks.

### B. DNS Threats

Tables V, VI, and VII summarize the DNS threats analyzed in Tables II–III. Each entry provides a one-line description of the threat and its potential impact. This concise representation highlights the diverse ways DNS can affect telephony service discovery, traffic steering, and slice-level operations in 5G/6G networks.

### C. Why Only Six Adversary Classes?

Our taxonomy deliberately limits itself to six adversary classes to balance expressiveness with analytical clarity. Introducing more granular roles—such as nation-state actors, malware operators, or specific insider subtypes—primarily refines motivation or scale rather than adding fundamentally new DNS capabilities. The six classes are distinguished by

*qualitatively different access paths* to DNS infrastructure and control-plane state.

Each class maps to a distinct capability boundary: network-level observation or manipulation ($A_1$, $A_2$); control over resolution infrastructure or naming authority ($A_3$, $A_4$); privileged operational access ($A_5$); and architectural leverage from multi-tenant or sliced deployments ($A_6$). Additional attacker roles can be treated as specializations or combinations of these classes without expanding the threat surface in a fundamentally new way.

This approach avoids overfitting the taxonomy to specific incidents or threat models while ensuring comprehensive coverage of DNS attack vectors in both legacy Internet and next-generation mobile networks.

### D. Realistic 5G/6G Deployment Assumptions

For our evaluation, we assume operational characteristics typical of current 5G networks and projected 6G architectures, reflecting how DNS is embedded within control-plane and service orchestration:

1) *Network Slicing and Multi-Tenancy:* Virtualized slices share physical infrastructure. Misconfigurations or attacks on shared DNS resolvers can propagate across tenants, impacting isolation and service availability.
2) *Service-Based Core and Discovery:* DNS mediates dynamic discovery of network functions, slice bootstrap, and mobility signaling. Resolution failures can cascade into service orchestration errors or traffic steering anomalies.
3) *Edge Deployments:* Edge-resident DNS caches and resolvers reduce latency but increase the attack surface. Local failures can propagate upstream, affecting multiple slices or tenants.
4) *Shared Resolver Dependencies:* Edge and core resolvers are often shared across services and slices, creating high-leverage points for cross-slice attacks.
5) *Partial DNSSEC and Encrypted DNS Deployment:* Legacy protocol support, permissive fallback behaviors, and incomplete DNSSEC deployment persist in operational networks, leaving known vulnerabilities exploitable.
6) *Tightly Coupled Control-Plane Dependencies:* DNS failures can simultaneously affect mobility, orchestration, traffic steering, and slice isolation. This coupling amplifies the impact of even minor misconfigurations or protocol weaknesses.

These assumptions underpin our threat evaluations, ensuring that severity ratings for service disruption, privacy leakage, amplification, traffic steering, slice impact, and misconfiguration risk are grounded in realistic deployment contexts.

### E. Configuration and Operational Misconfigurations

Category B captures DNS vulnerabilities arising from configuration errors and operational oversights, which are particularly consequential in complex 5G/6G deployments.

A representative example is *IMS ENUM Zone Misconfiguration* ($T_{32}$) [54], where errors in ENUM zone delegation, record provisioning, or namespace maintenance disrupt E.164-based service discovery for IMS. Unlike protocol-level integrity failures, this threat stems from configuration and lifecycle management mistakes—such as incorrect NAPTR records [132], [133], broken delegations, or stale ENUM entries—which directly affect SIP/IMS resolution paths in 5G/6G networks.

Under realistic deployment assumptions (please refer to Table II, row $T_{32}$), *service disruption* is *high* (●), because misconfigured ENUM zones can prevent call routing, break session establishment, or cause persistent registration failures. *Privacy leakage* is *medium* (◆), as misrouted queries or exposed ENUM records may reveal subscriber identifiers or service metadata without disclosing traffic content. *Amplification risk* is *low* (■), since misconfigurations typically remain scoped to specific zones or operators. *Traffic steering* is *medium* (◆), as incorrect ENUM mappings can redirect SIP signaling to unintended endpoints. *Impact on network slices* is *high* (●), reflecting the shared nature of IMS and ENUM services across slices, where a single configuration error can affect multiple tenants. Finally, *misconfiguration risk* is *high* (●), given the operational complexity of coordinating DNS operations, IMS provisioning, and regulatory numbering policies.

This threat is primarily exploitable by malicious or compromised infrastructure components ($A_3$), which can introduce or maintain faulty ENUM records, and by operational or administrative adversaries ($A_5$), such as errors introduced during maintenance or upgrades. It highlights how operational DNS errors—rather than cryptographic failures—can persistently undermine telephony reliability and control-plane integrity in 5G/6G IMS deployments.

For *IMS ENUM Zone Misconfiguration* ($T_{32}$) [54], misconfigured ENUM zones can lead to telephony service failures, including misrouted calls, incomplete IMS session setup, and inadvertent exposure of subscriber information. Such risks can be *mitigated* through (see Table IV, row $T_{32}$) automated zone validation, dependency-aware configuration, and slice-specific resolver isolation, which help prevent cascading failures across services. These controls should be enforced primarily at the core infrastructure to ensure consistent policy across operators, while edge-level checks can provide local safeguards and reduce immediate user impact.

The main trade-offs involve increased operational overhead, as administrators must maintain automated validation and dependency tracking, continuous monitoring to detect misconfigurations promptly, and inter-operator coordination to ensure consistent zone policies across networks. These measures can also introduce additional management complexity and require careful synchronization with legacy systems.

### F. Infrastructure and Control-Plane Dependencies

Category C highlights risks arising from shared DNS infrastructure and control-plane dependencies in multi-tenant 5G/6G

deployments.

A representative example is *Resolution Failures in the 3GPP Control Plane* ($T_{51}$) [54], where DNS resolution failures disrupt service discovery among control-plane network functions. Unlike Category A threats (protocol or cryptographic failures) or Category B threats (operator misconfigurations), this threat stems from *dependency and interaction failures* between DNS and tightly coupled control-plane components, including IMS, SBA functions, or ENUM-backed discovery mechanisms. Failures may arise from resolver unavailability, inconsistent resolution states, dependency loops, or fragile assumptions about DNS reachability in virtualized control planes.

Under realistic deployment assumptions (please refer to Table II, row $T_{51}$), *service disruption* is *high* (●), because control-plane functions depend on timely DNS resolution for registration, authentication, and session establishment; failures can block call setup, mobility management, or service binding. *Privacy leakage* is *medium* (◆), as repeated failed lookups or fallback behavior may reveal service identifiers, control-plane naming structures, or slice metadata without exposing user payloads. *Amplification risk* is *low* (■), since failures are generally scoped to specific dependency chains. *Traffic steering* is *medium* (◆), as partial resolution can redirect control-plane signaling to backup functions, degraded paths, or non-optimal service instances. *Impact on network slices* is *high* (●), reflecting the shared nature of DNS-based service discovery across slices. Finally, *misconfiguration risk* is *high* (●), due to complex interdependencies between DNS, orchestration systems, and control-plane functions.

$T_{51}$ [54] is exploitable by malicious or compromised infrastructure components ($A_3$), such as resolvers or control-plane services introducing inconsistent resolution behavior, and by operational or administrative adversaries ($A_5$), including errors during deployment, scaling events, or orchestration changes. This example demonstrates how even correctly configured and cryptographically sound DNS can become a critical point of failure when embedded in tightly coupled control-plane architectures.

This threat can be effectively *mitigated* (see Table IV, row $T_{51}$) through dependency-aware orchestration, resolver redundancy, state synchronization across core and edge components, and anomaly detection. These controls should be enforced primarily at the core infrastructure, with supplemental checks at the edge/MEC to limit localized impact. The main trade-offs include orchestration complexity, due to managing dependencies across core and edge components; the need for continuous monitoring to maintain synchronized resolver state; and cross-service coordination to ensure consistency across multiple network slices. Implementing these measures increases operational overhead and requires careful alignment with legacy network functions.

### G. Privacy, Metadata Leakage, and Surveillance

Category D captures threats that exploit observable patterns in DNS traffic or metadata, even when payload content is encrypted.

A representative example is *IMS Service Metadata Exposure via DNS* ($T_{69}$) [54], where DNS queries and responses for IMS service discovery inadvertently reveal metadata about mobile services, control-plane functions, or subscriber handling. In IMS deployments, DNS locates SIP servers, application servers, and service anchors via SRV, NAPTR, and related records. Even with encrypted payloads, these DNS interactions can expose service structure, deployment topology, or usage patterns to external observers.

Under realistic 5G/6G deployment assumptions (please refer to Table III, row $T_{69}$), *service disruption* is *medium* (◆), since metadata exposure alone does not directly block call setup or session establishment but may facilitate follow-on attacks. *Privacy leakage* is *high* (●), as observable DNS records and query patterns can reveal IMS service roles, numbering relationships, or coarse-grained subscriber and slice associations. *Amplification risk* is *medium* (◆), because leaked metadata can be correlated across multiple observations but does not automatically propagate system-wide. *Traffic steering* is *medium* (◆), as exposed service information can assist adversaries in targeting resolution paths without directly altering routing. *Impact on network slices* is *medium* (◆), reflecting that shared IMS infrastructure may leak slice distinctions without causing immediate cross-slice failures. *Misconfiguration risk* is *medium* (◆), as excessive metadata exposure typically stems from permissive DNS publishing rather than operational errors.

$T_{69}$ [54] is primarily exploitable by passive observers ($A_1$), who can infer IMS service structure, deployment decisions, or operational patterns by monitoring DNS traffic. This example illustrates how DNS, even when functioning correctly, can act as an information side channel in mobile control planes, emphasizing the need to minimize metadata exposure in 5G and emerging 6G IMS deployments.

An effective *mitigation* scheme (see Table IV, row $T_{69}$) involves minimizing record exposure, using split-horizon or private resolvers, enforcing access control, and applying rate limiting. These controls should be enforced primarily at the core infrastructure, with supplemental edge-level measures to reduce local exposure. The main trade-offs include operational overhead from managing fine-grained access controls, added latency introduced by filtering and rate-limiting mechanisms, and cross-slice coordination requirements to ensure consistent enforcement across multiple tenants. Implementing these measures also requires careful integration with legacy systems to maintain operational consistency.

### H. Software, API, and Implementation Vulnerabilities

Category E concerns flaws in resolver software or DNS-integrated APIs that can be exploited to disrupt resolution or compromise multiple slices.

A representative example is *Weak 5G Core DNS API Hardening* ($T_{76}$) [41], [58], where insufficient security controls on DNS-related APIs in the 5G core expose service discovery

and resolution mechanisms to abuse. In Service-Based Architectures (SBA), DNS functionality is increasingly accessed via APIs used by components such as the Network Exposure Function (NEF), CAPIF, and internal control-plane services. Weak authentication, inadequate authorization, or poor input validation in these APIs can allow unauthorized entities to manipulate resolution behavior or inject malformed requests, disrupting core network operations.

Under realistic 5G/6G deployment assumptions (please refer to Table III, row $T_{76}$), *service disruption* is *high* (●), because compromised APIs can interfere with service registration, discovery, or binding between core network functions, potentially causing widespread control-plane failures. *Privacy leakage* is *medium* (◆), as exposed APIs may reveal service identifiers, topology information, or operational metadata without necessarily exposing user-plane traffic. *Amplification risk* is *low* (■), since API-level abuse generally requires targeted access and does not automatically propagate across slices. *Traffic steering* is *medium* (◆), because API manipulation can influence how services locate or prioritize endpoints, even without direct control of routing. *Impact on network slices* is *high* (●), reflecting the shared nature of core DNS services and APIs, where a single vulnerable interface can affect multiple tenants. Finally, *misconfiguration risk* is *high* (●), due to the complexity of securing numerous interdependent APIs and the likelihood of persistent hardening gaps.

$T_{76}$ [41], [58] is exploitable by malicious or compromised infrastructure components ($A_3$), which may already have partial access to core services, and by operational or administrative adversaries ($A_5$), through insecure deployment or insufficient access controls. This threat illustrates how software and API hardening failures—rather than protocol flaws—can undermine DNS reliability and security in cloud-native 5G/6G cores.

Effective *mitigation* for this threat (see Table IV, row $T_{76}$) involves enforcing strong authentication and authorization, validating API inputs, applying rate limiting, and conducting regular security audits. These controls should be enforced primarily at the core infrastructure, with supplemental monitoring at the edge where appropriate. The main trade-offs include operational overhead from API hardening and auditing, added latency due to authentication and rate-limiting mechanisms, and cross-slice coordination requirements to ensure consistent enforcement across tenants. Implementing these measures also requires careful alignment with legacy systems and inter-operator processes.

### *I. DNS Integrity and Resolution Manipulation*

Category F covers threats that exploit resolver behaviors—such as caching, prefetching, or failover logic—to manipulate DNS resolution outcomes.

A representative example is *Resolver Failover Manipulation ($T_{84}$)* [59], where attackers abuse resolver redundancy and failover mechanisms to influence resolution paths. Modern mobile networks employ hierarchical and tiered resolver deployments to ensure resilience and low-latency access across core, edge, and slice-specific environments. However, failover logic—including health checks, timeout thresholds, or resolver prioritization—can be manipulated to suppress legitimate resolvers and force queries toward degraded or adversary-controlled alternatives.

Under realistic 5G/6G deployment assumptions (please refer to Table III, row $T_{84}$), *service disruption* is *medium* (◆), since failover manipulation typically degrades resolution intermittently rather than causing total outages. *Privacy leakage* is *medium* (◆), as redirected queries may expose service identifiers, timing patterns, or slice affiliation to unintended resolvers without revealing payload content. *Amplification risk* is *low* (■), because effects usually remain localized to resolver pools or domains. *Traffic steering* is *high* (●), as successful failover manipulation can systematically redirect queries toward adversary-influenced resolvers, enabling persistent observation or selective disruption. *Impact on network slices* is *high* (●), reflecting shared resolver infrastructure where failover decisions in common components affect multiple tenants. Finally, *misconfiguration risk* is *medium* (◆), due to overly aggressive failover thresholds, inconsistent health checks, or incomplete fallback validation.

$T_{84}$ [59] is exploitable by on-path adversaries ($A_1$), who can induce timeouts or packet loss, by malicious or compromised infrastructure components ($A_3$), which manipulate resolver behavior internally, and by operational or administrative adversaries ($A_5$), through misconfiguration of resolver priorities or failover policies. This example demonstrates how mechanisms intended to improve availability can become vectors for integrity and traffic-steering attacks in multi-slice mobile DNS deployments.

An effective *mitigation* scheme (see Table IV, row $T_{84}$) involves careful tuning of failover thresholds, consistent health checks, fallback validation, and monitoring for anomalous resolver behavior. Controls should be applied primarily at the DNS infrastructure and recursive resolvers, with edge/MEC oversight to detect and limit localized manipulation. The main trade-offs include operational overhead from implementing and maintaining these measures, added latency due to stricter failover policies, and increased monitoring complexity across slices.

**TABLE V:** A Taxonomy of Persistent DNS Threats in Future-Generation Mobile Networks (Categories A and B).

| ID | DNS Threat | Description |
|---|---|---|
| A: Protocol-Level and Cryptographic Weaknesses (Sec. V-A) | | |
| $T_1$ | DNS-over-TLS Certificate Misvalidation [48] | Improper certificate validation enables man-in-the-middle interception of encrypted DNS queries between mobile core and edge functions. |
| $T_2$ | DNS Cache Poisoning [49] | Forged responses injected into recursive resolvers can redirect subscribers or control-plane functions to attacker-controlled endpoints. |
| $T_3$ | Plaintext DNS Exposure [64] | Unencrypted queries allow passive adversaries to infer service usage, mobility, and application behavior in cellular networks. |
| $T_4$ | Incomplete DNSSEC Deployment [19] | Partial DNSSEC adoption leaves mobile core and edge resolution paths unsigned or unvalidated. |
| $T_5$ | DNSSEC Misconfiguration [65] | Broken trust chains or expired signatures cause validation failures or silent bypass, affecting mobile services. |
| $T_6$ | NXDOMAIN Hijacking [66] | Manipulated non-existent domain responses redirect traffic or inject content, disrupting service discovery. |
| $T_7$ | DNS Tunneling [67], [68] | Abuse of DNS queries/responses enables covert channels for data exfiltration or command-and-control. |
| $T_8$ | Long TTL Abuse [69] | Excessive TTL values delay recovery from compromise, prolonging incorrect routing in mobile networks. |
| $T_9$ | Resolver Capability Downgrade Attacks [50] | Forcing fallback from secure mechanisms weakens DNS resolution in service-based mobile architectures. |
| $T_{10}$ | DNSSEC Key Exhaustion [70] | Excessive validation triggers resource exhaustion in resolvers, degrading availability of mobile network functions. |
| $T_{11}$ | Algorithm Downgrade Attacks [50] | Forcing weaker cryptographic algorithms undermines DNS integrity relied upon by mobile services. |
| $T_{12}$ | Fragmentation-Based DNS Attacks [71] | Exploiting IP fragmentation in large responses allows forged records to be injected along mobile resolution paths. |
| $T_{13}$ | EDNS0 Abuse [18] | Misuse of EDNS0 inflates responses or triggers parser failures in resolvers across mobile and MEC environments. |
| $T_{14}$ | Protocol-Level DNS Downgrade Attacks [50] | Active interference forces fallback to insecure resolution paths used by mobile devices and network functions. |
| $T_{15}$ | Stale DNSSEC Key Retention [46] | Retaining retired keys increases replay and compromise risk in long-lived mobile deployments. |
| $T_{16}$ | DNSSEC Algorithm Downgrade [50] | Permissive validation policies weaken trust anchors for mobile services. |
| $T_{17}$ | *ENUM DNSSEC Integrity Failure* [54] | Misconfigured DNSSEC in ENUM domains allows spoofed responses, misrouting IMS sessions and calls in 5G/6G networks. |
| B: Configuration and Operational Misconfigurations (Sec. V-B) | | |
| $T_{18}$ | Misconfigured Wildcard Records [72], [73] | Overbroad wildcards expose unintended services or facilitate impersonation of mobile core and edge endpoints. |
| $T_{19}$ | Operational DNS Debt [42] | Legacy misconfigurations persist across network upgrades, virtualization, and slice reconfiguration. |
| $T_{20}$ | Insecure Bootstrap Resolvers [74] | Reliance on insecure or hardcoded resolvers during initialization weakens trust establishment for devices and network functions. |
| $T_{21}$ | Misconfigured Reverse DNS (PTR Records) [75] | Incorrect or missing PTR records undermine authentication, logging, and abuse detection. |
| $T_{22}$ | Registrar Account Takeover [76] | Compromised registrar accounts enable large-scale DNS record manipulation for operator-managed mobile domains. |
| $T_{23}$ | DNS Policy Inconsistency [77] | Divergent policies across regions, roaming domains, or slices cause unpredictable resolution behavior. |
| $T_{24}$ | Stale DNS Records [78] | Outdated resource records redirect traffic to decommissioned or reassigned infrastructure in mobile networks. |
| $T_{25}$ | Lame Delegations [79] | NS records pointing to non-authoritative or unreachable servers increase spoofing and DoS risk. |
| $T_{26}$ | Missing Response Rate Limiting (RRL) [43] | Absence of RRL on authoritative servers amplifies susceptibility to volumetric attacks targeting mobile services. |
| $T_{27}$ | Edge DNS Misconfiguration [63] | Improper deployment at edge or MEC nodes expands attack surface and reduces fault isolation for latency-sensitive services. |
| $T_{28}$ | Split-Horizon DNS Errors [80] | Inconsistent internal and external views expose internal services or disrupt access-network resolution. |
| $T_{29}$ | Lack of DNS Redundancy [52] | Single points of failure in authoritative or recursive DNS increase outage risk for mobile cores and edge services. |
| $T_{30}$ | Misconfigured Forwarders [81] | Forwarding queries to unreachable, untrusted, or misconfigured upstream resolvers degrades DNS reliability. |
| $T_{31}$ | Incorrect Glue Records [78] | Outdated or invalid glue records disrupt resolution for operator-managed domains. |
| $T_{32}$ | *IMS ENUM Zone Misconfiguration* [54] | Errors in ENUM zone delegation or record management misroute E.164-based service discovery, disrupting IMS call and session setup in 5G/6G networks. |
| $T_{33}$ | Broken Fallback Resolvers [82] | Secondary/backup resolvers fail to respond, causing resolution delays or outages for mobile core and edge services. |
| $T_{34}$ | IPv6 DNS Misalignment [83], [84] | Inconsistent IPv4/IPv6 records misroute traffic or weaken security in dual-stack mobile networks. |
| $T_{35}$ | Operational Visibility Gaps [85] | Limited monitoring or auditing obscures attacks, misconfigurations, or drift in distributed mobile infrastructures. |
| $T_{36}$ | Recursive Resolver Looping [86], [87] | Misconfigurations trigger recursive loops, amplifying traffic and degrading resolver performance for mobile functions. |

**TABLE VI:** A Taxonomy of Persistent DNS Threats in Future-Generation Mobile Networks (Categories C and D).

| ID | DNS Threat | Description |
|---|---|---|
| | C: Infrastructure and Control-Plane Dependencies (Sec. V-C) | |
| $T_{37}$ | Cross-Slice DNS Leakage [61] | Insufficient isolation leaks queries or cached responses across network slices, violating slice security boundaries. |
| $T_{38}$ | Control-Plane DNS Dependence [88] | Tight coupling of control-plane functions to DNS causes failures to cascade into signaling or service outages. |
| $T_{39}$ | Weak Access Controls on DNS APIs [89] | Inadequate authentication/authorization allows unauthorized changes to DNS records used by mobile services. |
| $T_{40}$ | DNS-Based Service Discovery Failures [47], [90] | Failures in DNS service discovery disrupt resolution of network functions in service-based architectures. |
| $T_{41}$ | Network Function Resolution Poisoning [47] | Corrupted DNS mappings misdirect signaling/data-plane traffic, causing service disruption. |
| $T_{42}$ | Slice Bootstrap DNS Failures [30] | Resolution failures during slice initialization prevent service instantiation or connectivity. |
| $T_{43}$ | Open Recursive Resolvers [91] | Public resolvers within operator networks enable reflection attacks and expose internal naming structures. |
| $T_{44}$ | Dependency on Third-Party DNS [92] | Reliance on external DNS introduces availability, supply-chain, and jurisdictional risks. |
| $T_{45}$ | DNS-Based Traffic Steering Abuse [62] | Manipulation of DNS load balancing or geolocation reroutes mobile traffic through adversarial or suboptimal paths. |
| $T_{46}$ | Resolver Trust Assumptions [88] | Overreliance on upstream resolvers without validation/redundancy creates single points of failure. |
| $T_{47}$ | Core Network DNS Flooding [93] | High-rate query floods target DNS-dependent 5G/6G core functions, degrading performance. |
| $T_{48}$ | Misaligned DNS Load Balancing [94] | Incorrect DNS load balancing overloads core, edge, or slice resources, violating SLAs. |
| $T_{49}$ | Cross-Tenant Resolver Contamination [53] | Shared resolver caches leak queries or records across tenants and slices. |
| $T_{50}$ | DNS Dependency Loops [95] | Circular dependencies among zones/resolvers cause failures affecting service continuity and control-plane functions. |
| $T_{51}$ | *Resolution Failures in 3GPP Control Plane* [54] | Failures in ENUM-based E.164 resolution disrupt control-plane service discovery and IMS call/session setup. |
| | D: Privacy, Metadata Leakage, and Surveillance (Sec. V-D) | |
| $T_{52}$ | Excessive DNS Logging [96] | Overcollection or prolonged retention of DNS logs exposes subscriber metadata and mobility behavior. |
| $T_{53}$ | WebRTC DNS and IP Leakage [97] | STUN/TURN interactions reveal real IP addresses or DNS-resolved endpoints, undermining privacy. |
| $T_{54}$ | DNS Query Fingerprinting [60], [98] | Analysis of query patterns uniquely identifies devices, applications, or users across mobile sessions. |
| $T_{55}$ | Encrypted SNI Correlation [99] | Correlation of DNS queries with encrypted SNI or timing reveals accessed services. |
| $T_{56}$ | Resolver-Side Profiling [100] | Resolvers or upstream providers profile users using DNS telemetry from mobile access networks. |
| $T_{57}$ | DNS Hijacking [101], [102] | Unauthorized record changes redirect mobile traffic via compromised registrars or control planes. |
| $T_{58}$ | Anycast Manipulation [103] | Abuse or misconfiguration of anycast DNS attracts traffic to adversarial or suboptimal locations. |
| $T_{59}$ | Anycast Routing Abuse [51] | Routing-layer manipulation of anycast paths diverts DNS traffic for interception or disruption. |
| $T_{60}$ | GeoDNS Abuse [104] | Exploitation of geographic responses selectively targets regions, roaming domains, or edge deployments. |
| $T_{61}$ | ISP-Level NXDOMAIN Rewriting [105] | NXDOMAIN modification injects redirects, monitoring, or censorship into mobile DNS resolution. |
| $T_{62}$ | DNS Enumeration [106] | Zone walking or brute-force queries reveal internal services, functions, or identifiers. |
| $T_{63}$ | DNS over HTTPS Policy Bypass [107] | DoH circumvents carrier DNS monitoring, filtering, or policy enforcement. |
| $T_{64}$ | Encrypted DNS Traffic Analysis [44], [45] | Timing, size, or destination metadata leaks behavioral information about mobile users. |
| $T_{65}$ | DNS-Based Service Enumeration [108], [109] | Systematic probing identifies exposed services, APIs, or management endpoints. |
| $T_{66}$ | Resolver Cache Snooping [96], [110] | Inference of other users' queries by probing shared resolver cache state. |
| $T_{67}$ | DNS-Based Covert Signaling [111], [112] | Low-bandwidth signaling via DNS timing or query patterns enables covert coordination. |
| $T_{68}$ | DNS Logging Jurisdictional Risk [113], [114] | Exposure of DNS logs to foreign legal regimes due to cross-border storage and roaming. |
| $T_{69}$ | *IMS Service Metadata Exposure via DNS* [54] | DNS queries for ENUM-based IMS services leak metadata about user sessions or service usage. |

**TABLE VII:** A Taxonomy of Persistent DNS Threats in Future-Generation Mobile Networks (Categories E and F).

| ID | DNS Threat | Description |
|---|---|---|
| E: Software, API, and Implementation Vulnerabilities (Sec. V-E) | | |
| $T_{70}$ | Insecure Dynamic DNS Updates [115] | Weak authentication or authorization allows unauthorized record changes, affecting distributed mobile services. |
| $T_{71}$ | Resolver Software Vulnerabilities [116] | Exploitation of implementation bugs causes crashes, DoS, or remote code execution, impacting core and edge resolution. |
| $T_{72}$ | Memory Corruption Bugs [117] | Use-after-free, buffer overflow, or parsing flaws in DNS libraries disrupt mobile service discovery and resolution. |
| $T_{73}$ | API Token Reuse [89] | Leaked or reused DNS management tokens enable persistent unauthorized access to DNS control planes. |
| $T_{74}$ | Orchestrator–DNS Desynchronization [118] | State inconsistencies between orchestration systems and DNS cause stale records or misrouting in cloud-native mobile deployments. |
| $T_{75}$ | Resolver Fingerprinting [119] | Inference of resolver type or configuration via crafted queries enables targeted exploitation in mobile deployments. |
| $T_{76}$ | *Weak 5G Core DNS API Hardening* [41], [58] | Insufficient input validation or authentication in SBA/NEF/CAPIF APIs exposes DNS service discovery endpoints to spoofing or injection, degrading resolution or service binding. |
| F: DNS Integrity and Resolution Manipulation (Sec. V-F) | | |
| $T_{77}$ | DNS Rebinding Attacks [120], [121] | Short TTLs remap domains to internal IPs, enabling cross-origin access to internal or edge services. |
| $T_{78}$ | Resolution-State Manipulation [122] | Altering resolver state or response handling changes resolution outcomes, affecting service routing without record compromise. |
| $T_{79}$ | Negative Caching Abuse [123] | Manipulating NXDOMAIN or SERVFAIL caching suppresses service reachability, disrupting mobile network access. |
| $T_{80}$ | TTL Manipulation Attacks [18], [124] | Malicious TTL inflation or reduction destabilizes traffic steering and prolongs incorrect mappings. |
| $T_{81}$ | Malicious DNS Prefetching [125] | Abuse of prefetching primes caches with attacker-controlled domains or overloads resolvers in mobile deployments. |
| $T_{82}$ | DNS-Based Phishing Infrastructure [126] | Fast-flux or short-lived domains support phishing campaigns targeting mobile users and services. |
| $T_{83}$ | DNS Shadowing [127] | Attacker-controlled subdomains persist unnoticed under legitimate domains, potentially misdirecting mobile traffic. |
| $T_{84}$ | *Resolver Failover Manipulation* [59] | Interference with failover redirects queries to malicious servers or induces service disruption in tiered resolver stacks. |