OECD publishing

SECURITY OF THE DOMAIN NAME SYSTEM (DNS)

AN INTRODUCTION FOR POLICY MAKERS

OECD DIGITAL ECONOMY PAPERS
October 2022 **No. 331**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report on "Security of the Domain Name System (DNS): an Introduction for Policy Makers" was prepared jointly by the OECD Working Party on Security in the Digital Economy (WPSDE) and Working Party on Communication Infrastructure and Services Policy (WPCISP), of the Committee on Digital Economy Policy (CDEP). It aims to inform policy makers about the current challenges and opportunities related to the digital security of the Domain Name System (DNS). This report should be read in conjunction with the accompanying report on "Security of Routing".

This report was drafted by Ghislain de Salins with contributions from Laurent Bernat, Verena Weber and Lauren Crean from the OECD Secretariat, and by WPSDE and WPCISP delegates. It was prepared under the supervision of Laurent Bernat and Verena Weber. It was approved and declassified by written procedure by the Committee on Digital Economy on 22 August 2022, and prepared for publication by the OECD Secretariat.

The Secretariat wishes to thank the external experts who contributed to the development of this report including, inter alia: Joe Abley; Einar Bohlin; Stéphane Bortzmeyer (Afnic); Chris Boyer (AT&T); Chris Buckridge; Graeme Bunton (DNS Abuse Institute); Gemma Carolillo (European Commission); David Conrad (ICANN); Cameron Dixon (DHS); Patrik Fältström (Netnod); Laurent Ferrali (ICANN); Marco Hogewoning; Geoff Huston (APNIC); Anne-Rachel Inné; Merike Kaeo; Olaf Kolkman (ISOC); Elena Plexida (ICANN); Paul Rendek; Andrei Robachevsky (ISOC); Chelsea J. Smethurst (Microsoft); Mark Svancarek (Microsoft); Bill Woodcock (PCH), and Suzanne Woolf (PIR).

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/CISP/SDE(2021)5/FINAL.

Table of contents

Figures

Boxes

Executive summary

The Domain Name System (DNS) is an essential logical infrastructure that enables the mapping of names and services on the Internet and underpins its very functioning. In fact, almost every activity on the Internet starts with a DNS query, i.e. a request for information sent by a user's machine to a DNS server. As a result, the impact of incidents affecting the DNS can be significant. They include digital security attacks, i.e. incidents caused intentionally by malicious actors (e.g. DNSpionage and the Sea Turtle DNS hijacking in 2018 and 2019), as well as unintentional incidents, for instance resulting from a misconfiguration that would make a DNS server unavailable (e.g. the Facebook outage in October 2021).

This report focuses on DNS security, i.e. the area of digital security that covers incidents disrupting the availability, integrity and confidentiality (the "AIC triad") of parts of the DNS ecosystem. It does not discuss areas beyond this scope such as certain forms of "DNS abuse".

Each actor in the DNS ecosystem, and each relationship between those actors, contain potential vulnerabilities that can be exploited by malicious actors or lead to an unintentional digital security incident. The report looks at three types of vulnerabilities whose exploitation may affect the AIC triad of the DNS ecosystem, as well as at the existing efforts and emerging solutions to address them:

- **"DNS-specific" vulnerabilities**, which result from flaws in the DNS protocol, its original design as well as its implementation, enabling for instance DNS spoofing and cache poisoning. Key technical developments to address those include DNS Security Extensions (DNSSEC) and encrypted DNS transport, e.g. DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH).
- **Vulnerabilities of DNS actors**, which may result from code vulnerabilities, misconfigurations, insufficient access controls and the human factor (e.g. social engineering), and include supply-chain attacks that may compromise registries and registrars. Key initiatives to address those include the mainstreaming of registry lock and zero trust approaches across the DNS ecosystem.
- **Dependencies and emerging concentration,** which could have significant consequences for DNS security (e.g. single points of failure with the risk of cascading effects).

The analysis highlights six common misconceptions about the DNS ecosystem and DNS security:

- **First misconception: the DNS is *only* a phonebook for the Internet**. Beyond the protocol that enables the translation (or "resolution") of human-readable names into machine-readable IP addresses, the DNS is an essential infrastructure that provides stables references on the Internet.
- **Second misconception: the importance of the DNS is decreasing**. Mobile applications and emerging technologies such as the Internet of Things (IoT), like almost any activity on the Internet, extensively rely on the DNS ecosystem, the importance of which is increasing in line with the digital transformation.
- **Third misconception: the DNS is an easy-to-understand and highly centralised system managed by ICANN**. The DNS is a complex ecosystem that combines some centralised functions with a highly distributed structure, which relies on thousands of systems and organisations across the world as well as on interactions with other systems and protocols.

- **Fourth misconception: easy fixes are available to solve DNS security issues**. There are often trade-offs between digital security and other key economic and social objectives such as technical performance, usability or profitability. Even within the realm of DNS security, technical solutions such as DNSSEC and encrypted DNS transport come with trade-offs.
- **Fifth misconception: nothing can be done to enhance DNS security**. Many initiatives have been launched by the multi-stakeholder community to enhance DNS security. They include economic incentives to support DNSSEC deployment, tools to better measure DNS security and solutions to enhance the confidentiality of DNS queries and user privacy.
- **Sixth misconception: DNS security is only a technical issue calling for technical remedies**. Economic factors such as misaligned market incentives play a key role in DNS security gaps. While technical solutions are the most effective means to fix vulnerabilities in the DNS protocol itself, their implementation, or lack thereof, are interrelated with economic and social incentives affecting DNS actors.

The role of governments in enhancing the digital security of the DNS ecosystem

Because the DNS is a key infrastructure that supports the very functioning of the Internet, there is a need for governments to better understand and prioritise DNS security. Enhancing DNS security should be considered as a co-operative journey, and the efforts of the multi-stakeholder community in this direction as an on-going process of innovation to better mitigate risk, in a constantly evolving environment.

In general, digital security measures may impact one dimension of the AIC triad positively, while negatively impacting another. DNS security is no exception: there is no panacea that would make the DNS entirely secure, and promising technical solutions often come with trade-offs. For both policy makers and actors of the DNS ecosystem, effective digital security policies and measures should aim to reduce digital security risk to an optimal level rather than to avoid the risk or seeking to entirely eliminate it and achieve “100% security”. **Policy makers therefore need to exercise caution** when introducing policies or initiatives to enhance DNS security, in order to avoid well-intentioned but ill-designed regulations that may lead to adverse effects. In particular, policy makers could significantly benefit from:

- **Consulting the DNS multi-stakeholder community and co-designing initiatives** regarding DNS security with its members. In particular, governments could work together with their ccTLDs to better measure and incentivise the adoption of DNS security best-practices such as DNSSEC signing, and with local ISPs to further develop DNSSEC validation and the use of encrypted DNS transport in their DNS resolution services;
- **Leading by example** with their own DNS infrastructure (e.g. by deploying DNSSEC signing for the authoritative DNS servers managed by the government);
- **Supporting stakeholder-led initiatives** to develop capacity building on DNS security, in particular targeting smaller organisations such as certain Internet Service Providers (ISPs), ccTLDs and registrars;
- **Promoting diversification** of the DNS ecosystem and its supply chain, in particular through the development of alternatives for key functions (e.g. DNS management software or resolvers);
- **Supporting research and development** in areas where significant technical gaps for DNS security remain unaddressed;
- **Co-operating at the international level** to enhance the security of the DNS ecosystem, preserve its functioning as a core global infrastructure and avoid Internet fragmentation. In that regard, enabling an international and multi-stakeholder dialogue to better understand and address DNS security challenges is essential.

Security of the Domain Name System (DNS): an introduction for policy makers

Introduction

Enhancing the digital security of communication networks is critical to strengthen trust in the ongoing digital transformation and to ensure the smooth functioning of our digitally dependent economies and societies. The COVID-19 pandemic highlighted the crucial role played by communication networks in enabling economic and social resiliency, in particular as organisations in many OECD countries switched to teleworking to ensure business continuity during lock-down orders.

The Domain Name System (DNS) is a key component of the logical infrastructure that supports the functioning of communication networks and of the Internet. From its development in the 1980s to the 2000s, the DNS was mostly considered by policy makers as a technical (as opposed to strategic) aspect of the functioning of the Internet. However, since the 2000s, governments have increasingly perceived the DNS as a potential point of control over the Internet and as a means to achieve various policy objectives, often at the content layer (e.g. using DNS filtering to prevent access to illegal content, including censoring content for political reasons). In parallel, it has also become clear that policy actions at the DNS level can have unintended consequences and even cause harm in areas distinct from the initial policy objective (e.g. in the area of digital security, DNS filtering may reduce availability or confidentiality for certain user categories) (SSAC, 2011[1]).

As a result, there has been a growing interest by policy makers in understanding how the DNS works, elevating it from a technical issue mostly discussed by engineers to a key public policy topic, now mentioned in high-level policy documents such as national cyber security strategies. In 2018, the Global Commission on the Stability of the Cyberspace highlighted the need to protect the DNS as part of the "public core" of the Internet (GCSC, 2018[2]). In its new cybersecurity strategy, the European Union noted an "increased reliance on the core functions of the global and open Internet, such as the DNS" (European Commission, 2020[3]) and listed "Internet security", with a focus on the DNS, as a key priority, alongside the security of mobile networks and of the Internet of Things (IoT). From another perspective, in the Russian Federation, a recently adopted law, Russian Federal Law N90-FZ, often referred to as the "Sovereign Internet Law", called for the establishment of a "national domain name system" (ICANN, 2021[4]).

The increased interest of policy makers in the DNS and its security results from a growing awareness of its criticality. Because the DNS is a foundational part of the logical infrastructure of the Internet (ICANN, 2019[5]), digital security incidents that affect its availability, integrity or confidentiality can have a significant impact on society as a whole. This relationship is highlighted by the frequent appearance of DNS digital security incidents in the headlines. In 2018, the "DNSpionage" attack saw the hijacking of the domain names of several organisations in the Middle East, including the Lebanese Ministry of Finance (Cisco, 2018[6]). In 2019, in the "Sea Turtle" attack, malicious actors launched supply-chain attacks targeting part of the DNS ecosystem such as registrars, registries (including Armenia's top-level domain, ".am") and

authoritative servers to gain access to the networks and systems of their final victims (Wired, 2019[7]). In both cases, the attacks were attributed to State-sponsored actors, or Advanced Persistent Threats (APTs), which compromised part of the DNS ecosystem to steal sensitive data from their targets.

More recently, in October 2021, the outage of Facebook and its subsidiaries became evident when DNS servers around the world failed to resolve Facebook's domain names. While the root cause of the outage was attributed to an update that led to a routing misconfiguration affecting Facebook's BGP (Border Gateway Protocol) announcements[1], tightly-coupled internal automation led to the disconnection of their DNS servers from the Internet (Madoury, 2021[8]; Facebook, 2021[9]). The Facebook outage shows that i) beyond malicious attacks, unintentional digital security incidents can have severe economic and social consequences too, and ii) the various protocols that form the logical layer of communication networks are intertwined and interdependent, resulting in a very complex overlay that can easily fail, as it is as strong as its weakest link. In the security community, "it's always DNS" has even become a popular meme, highlighting that network incidents often result from vulnerabilities of the DNS ecosystem, including for instance DNS misconfigurations.

While there is a growing awareness of policy makers on the need to better understand and manage the digital security of the DNS, the existing literature tends to focus either on the technical aspects of DNS security or on geopolitical concerns. The purpose of this report is precisely to go beyond these two aspects and to rather favour a holistic approach, focusing on economic and social aspects. In this context, the report aims to clarify and address the legitimate questions policy makers may have about the DNS and its security: how does it work? Who are the main actors in the DNS ecosystem? Is it secure enough? Are there best practices or success stories that deserve more attention? What should be the role – if any – of policy makers in enhancing DNS security?

Objectives and audience

This report is intended to be informational and educational. Its main objective is to provide a high-level overview of the key challenges and opportunities associated with the security of the Domain Name System (DNS).

The target audience of this report is the community of policy makers involved in digital security, telecommunications and the digital transformation more broadly. As it is addressed to policy makers, this report does not intend to discuss in-depth technical details related to the DNS and its security.

This report was drafted on the basis of desk research by the OECD Secretariat, as well as of interviews conducted with stakeholders from various countries and communities, including governments, businesses, civil society and the technical community.

Scope

Today's communication networks are complex ecosystems, often described as an overlay of multiple physical and logical layers[2]. Within the broader OECD work stream on the digital security of communication networks, this report focuses on the security of the DNS, which is one of the key protocols used at the logical layer.

This report should be read in conjunction with the reports on digital security of communication networks' infrastructure, which focuses on the physical layer [DSTI/CDEP/CISP/SDE(2021)3], and on security of routing, which is another key building block of the logical layer [DSTI/CDEP/CISP/SDE(2021)4].

This report focuses on the digital security incidents that have a technical impact on the DNS, i.e. that affect the availability, integrity or confidentiality of part of the DNS ecosystem.

As further outlined below, the report does not extensively discuss DNS abuse, i.e., in the context of this report, the use of the DNS for malicious purposes, which can include digital security attacks (e.g. using the DNS for phishing or spreading malware) or sharing illegal content. This definition does not necessarily reflect an international consensus. In fact, the scope and definition of DNS abuse remain a topic of debate within the multi-stakeholder community. The role of the DNS in content regulation (e.g. intellectual property protection, hate speech, disinformation), which is relatively limited and often misunderstood, as well as geopolitical considerations regarding the DNS are also considered out of the scope of this report.

With this context in mind, this report will first discuss key concepts of digital security risk management (section 1), and outline what the DNS is as well as the main actors in the DNS ecosystem (section 2). It will then discuss DNS security and how it should be differentiated from DNS abuse (section 3). The sections that follow discuss the key vulnerabilities of the DNS ecosystem (section 4) as well as existing efforts and emerging solutions to mitigate those (section 5). Finally, the report will outline some key insights for policy makers (section 6).

1. What is digital security?

Digital security is the set of measures taken to manage digital security risk, which is the detrimental effect that digital security incidents can have on economic and social activities. Digital security risk is usually measured in terms of likelihood and impact. At the technical level, the impact of digital security incidents is usually defined through three dimensions: the availability, integrity and confidentiality of data, networks, software and hardware. These three dimensions are also referred to as the "AIC triad". Beyond this technical impact, digital security incidents have economic and social consequences, which can be severe (e.g. the unavailability of a company's domain name may entirely disrupt its business operations, internal communications, etc.).

With the digital transformation, economic and social activities, including critical ones (e.g. healthcare, transport) are increasingly reliant on the Internet. Because the DNS is an essential logical infrastructure that underpins the functioning of the Internet, the impact of incidents affecting the DNS can be significant. Such incidents include digital security attacks, i.e. intentional incidents caused by malicious actors, for instance in the case of the Sea Turtle DNS hijacking (Wired, 2019[7]). Digital security incidents may also be unintentional, resulting from a power outage or a misconfiguration that would make a DNS service unavailable, for instance in the case of the Facebook outage in October 2021 (Facebook, 2021[9]; Madoury, 2021[8]).

The goal of digital security is to manage digital security risk, i.e. to reduce the likelihood and impact of digital security incidents, while recognising that 100% security cannot be achieved. Many digital security measures come with trade-offs and may negatively impact other aspects of the economic and social activities at stake. For instance, security measures may affect technical performance or increase costs. They may also positively impact one dimension of security while negatively impact another: security measures that may increase data confidentiality could also reduce their availability. Historically, the design and evolution of the DNS ecosystem have prioritised its availability, adaptability and tolerance to variant behaviours and configurations, rather than other dimensions such as integrity and confidentiality.

DNS security is no exception, and technical measures that may enhance integrity or confidentiality could also reduce availability, significantly increase costs or affect usability. In other words, there is no "silver bullet" (i.e. a perfect solution) that would make the DNS ecosystem entirely secure. As a result, for both policy makers and actors of the DNS ecosystem, effective digital security policies and measures should aim to reduce digital security risk to an optimal level rather than to avoid it or entirely eliminate it. [3]

As for other digital security incidents, DNS security incidents result from a combination of vulnerabilities and threats:

- Vulnerabilities are weaknesses which, if exploited, can lead to a digital security incident. They include code vulnerabilities, lack of access control measures (e.g. weak passwords or unauthenticated protocols) and human error (e.g. susceptibility to phishing or misconfigurations).
- Threat actors are entities willing to exploit vulnerabilities to cause harm, and range from relatively unskilled individuals ("script kiddies") and more experienced hackers that are ideologically motivated ("hacktivists") to organised criminal groups[4] and State-sponsored actors, often referred to as Advanced Persistent Threats (APTs). In recent years, there has been an increasing interest of APTs in targeting the DNS, as exemplified in recent attacks such as DNSpionage (Cisco, 2018[6]; Mercer and Rascagneres, 2019[10]). Threat actors use threat vectors, i.e. tools and techniques designed to carry out attacks.

Finally, as both vulnerabilities and threats evolve constantly, managing digital security risk is often considered a journey: the efforts of the multi-stakeholder community to enhance security contribute to an on-going process of innovation to better mitigate digital security risk, in a constantly evolving environment.

2. What is the DNS?

This section provides an introduction to the DNS ecosystem and aims to enable policy makers to understand DNS fundamentals in view of the discussion below regarding DNS security.

What the DNS is not

To start with, three common misconceptions about the DNS should be highlighted.

- **First misconception: the DNS is *only* a phonebook for the Internet**.

The DNS is often described as the protocol (i.e. an agreed set of rules to standardise data formats and processing) – and as the ecosystem that implements that protocol – which enables the translation (or "resolution") of human-readable names (i.e. that are easy to read and remember, such as www.oecd.org) into machine-readable IP addresses (e.g. 78.41.128.129). While this definition has its merits (and is not incorrect *per se*), it also wrongly suggests that the Internet could easily function without the DNS, as devices may simply use IP addresses to talk to each other.

In fact, almost any activity on the Internet, including for instance email exchanges, heavily relies on the DNS and depends on it to function properly. In today's Internet architecture, the DNS also plays an important role in load-balancing and localisation of traffic. It is a common strategy for many Content Delivery Networks (CDN) and cloud providers to use the DNS to steer clients to a particular local instance for a service or to select which data centre to contact.

Another commonly held misconception is that to each device is assigned a unique and permanent IP address. However, IP addresses are often allocated to devices in a dynamic manner, and may even be used as "ephemeral tokens" only attributed within the context of a session. IP addresses attributed to devices or services are likely to change over time. In contrast, a domain name provides a stable reference for locating a device or a service on the Internet. Thus, while a domain registrant may switch web-hosting providers and consequently receive a different IP address for their website, the domain name will remain unchanged, even as it transparently points to the new provider. In other words, domain names provide stable references on the Internet, and the DNS enables a mapping from a name to the coordinates of a service delivery point on the Internet, allowing user (or "client", as opposed to "server") applications reliably connect to services.

Beyond its "name-to-address translation" function, the DNS could be described as a fundamental infrastructure that supports networks' "rendezvous function" between user applications and services. The DNS is in fact "one of the most important infrastructure components of the Internet" as "almost every activity on the Internet starts with a DNS query" (IETF, 2021[11]).

- **Second misconception: the importance of the DNS is decreasing**, because of the increased use of keyword search and mobile applications as well as of the development of the Internet of Things (IoT).

As a corollary of the first misconception, the second misconception notes that humans are less and less likely to type domain names in a browser or in emails, as they increasingly access content through mobile applications. Similarly, IoT devices may exchange data without the need for human intervention (hence, for human-readable names) through machine-to-machine (M2M) communication. Nevertheless, and for the reason stated above (DNS "rendezvous function"), these use-cases heavily rely on the DNS for their functioning.

In fact, for both IoT and mobile applications, domain names are not used for their human-friendliness but rather for the mapping and stable references they provide on the Internet. Therefore, the importance of the DNS is increasing in line with the digital transformation, as most Internet applications rely on the DNS for functioning.

- **Third misconception: the DNS is a simple and centralised system managed by ICANN**.

The Internet Corporation for Assigned Names and Numbers (ICANN) has indeed some limited centralised role for key functions such as developing policies for and managing the assignment of generic top-level domains (gTLDs), and enabling co-ordination between some actors of the multi-stakeholder community. However, the DNS ecosystem more broadly is highly distributed complex, as it relies on thousands of systems and organisations across the world. This ecosystem is all the more complex as its functioning relies on interactions with other systems and protocols such as the Border Gateway Protocol (BGP) (see [DSTI/CDEP/CISP/SDE(2021)4]).

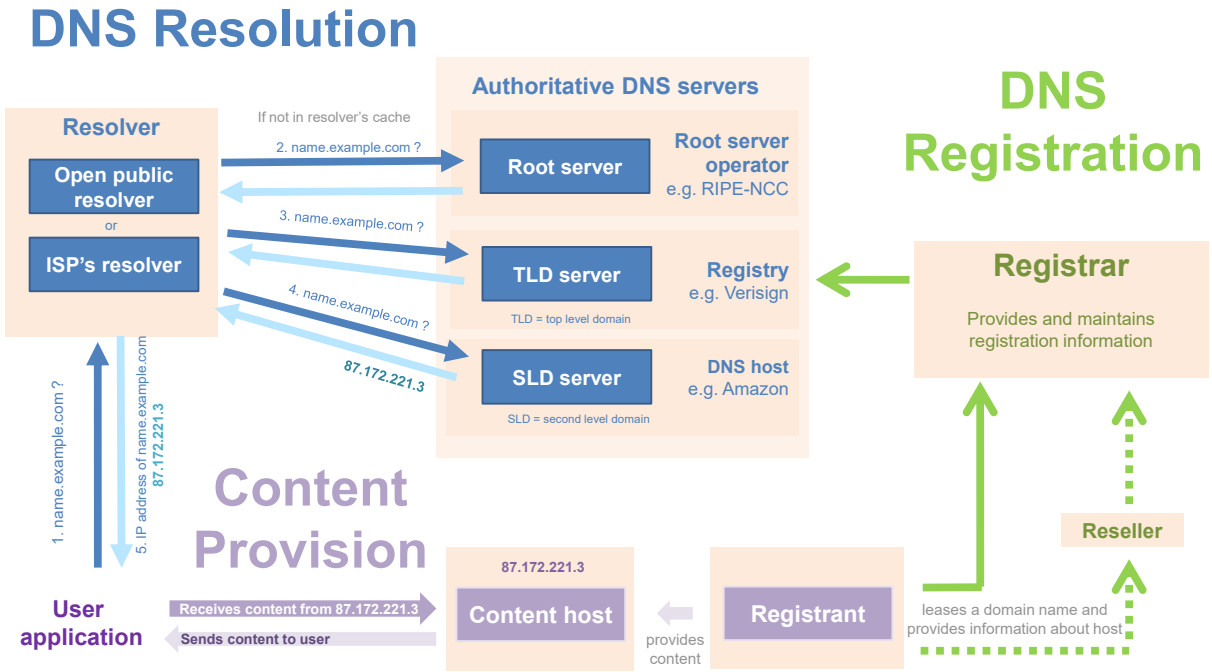
In fact, the DNS ecosystem is a complex structure, which is both centralised in some aspects (e.g. certain functions operated by ICANN) and highly distributed in others, as further described below.

A complex ecosystem

With these caveats in mind, the DNS can be described as a fundamental logical infrastructure upon which the Internet is critically dependent for its functioning (ICANN, 2019[5]). More precisely, the DNS is a highly complex ecosystem that enables the mapping of names and services on the Internet. The structure of this ecosystem is both centralised in some aspects and globally distributed in others, as a wide variety of stakeholders contribute to its functioning.

This ecosystem enables the practical implementation of the DNS query-response protocol, which was designed in the 1980s but has been significantly extended and improved since, notably through the many RFCs (Requests for Comments) developed by the Internet Engineering Task-Force (IETF). The DNS also underpins the universality of the Internet, as the unique identifiers it provides enable user applications – wherever they are in the world – to receive the same predictable results when accessing a domain name. Within this ecosystem, two important processes are at play and enable the DNS to function (see Figure 1).

Figure 1. Overview of the DNS resolution and registration process



Note: This high-level overview does not intend to be exhaustive, but rather to provide a simplified picture of the processes at play in the DNS.

Dotted lines represent alternative or optional paths.
Source: OECD

These two processes are:

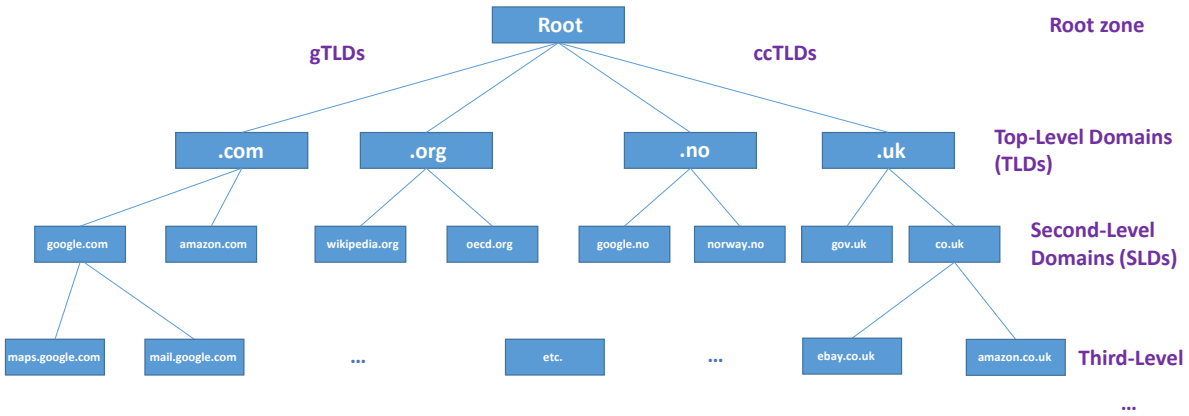
- The registration process, which enables a registrant to lease[5] a domain name, i.e. buy an exclusive right-of-use of a domain name for a specified period, typically one year). This process typically involves a registrant, a registry and a registrar. It could be described as the "supply-side" of the DNS ecosystem (i.e. regarding the individual or organisation that provides services or content, e.g. through a website associated with a domain name).
- The resolution process, which enables a user application to access services or content by means of a DNS resolution. This process typically involves a user (or "client", as opposed to a "server") application, a resolver and authoritative DNS servers (including root servers, registries or top-level servers, second-level servers, etc.). It could be described as the "demand-side" of the DNS ecosystem (i.e. regarding the user application that intends to access services or content). As outlined in Figure 1, to resolve a domain name into an IP address, the resolver can either:
  - Use the information already cached (i.e. stored within the resolver database, usually for a short period called Time-to-Live or TTL): if the same domain name has been queried recently, the resolver already has the IP address corresponding to the domain name.
  - Initiate a DNS query, starting at the top of the hierarchical architecture of the DNS name space (or the right of the domain name as it appears on a browser), with the root, down to the top-level domain (TLD), the second-level domain (SLD) and below, where appropriate (e.g. third-level domains). If the responses to these search queries are already cached by the resolver, the locally cached information is used to speed up the process.

Importantly, the DNS ecosystem belongs to the logical layer, which exists and operates independently from the websites or services that provide content (I&J, 2021[12]).

To enable these two processes to function, the DNS name space is structured in a hierarchal manner that can be mapped into a distributed database, relying on different managed areas or "zones". The root zone is at the very top of that hierarchy, as outlined in Figure 2. Below the root are top-level-domains, or TLDs, managed by registries. Below registries are second-level domains, or SLDs. On a domain name as it appears in a browser (e.g. "amazon.co.uk"), the hierarchy starts on the right with the root, followed by the TLD, SLD and lower levels.

Each TLD may design and implement specific registration policies, e.g. regarding the purpose or content of domain names registered under the TLD and SLDs, or regarding attributes of the registrants. Some country-code TLDs (ccTLDs) have developed SLDs dedicated to specific purposes, e.g. commercial entities for "co.uk". For the ".fr" ccTLD, the registration charter (or "charte de nommage") requires that registrants reside in the European Union (EU), the European Economic Area (EEA) or Switzerland (Afnic, 2021[13]). When they are well designed and sufficiently enforced, such policies can be an important tool to address DNS abuse, e.g. by clearly formalizing registration rules and processes to handle conflicts (see Annex B).

Figure 2. The hierarchical structure of the DNS name space



Note: Each block on the figure corresponds to a DNS zone. The hierarchy starts with the root, down to TLDs, SLDs and levels below. The description above does not intend to be exhaustive (1589 TLDs are active as of October 2021).
Source: OECD

Main actors of the DNS ecosystem

To enable the DNS ecosystem to function, the following actors (later referred to as "DNS actors'') play a key role.

For the resolution process

The resolution process enables user applications to resolve or translate a domain name into an IP address. It involves two distinct types of DNS servers: authoritative servers on one hand, and resolvers on the other hand.

- The **authoritative DNS servers** store key information for the functioning of the DNS, including lists of domain names and associated IP addresses, and respond to queries from resolvers:
  - While not considered an authoritative server *per se*, the **Internet Assigned Numbers Authority (IANA)** manages the DNS root zone, including the assignment of top-level domains (TLDs). The IANA is operated by ICANN.
  - **Root servers** (or rootname servers) are authoritative servers for the root zone of the DNS. They answer queries for records in the root zone and return addresses for authoritative name servers for top-level domain (TLDs). There are 13 root servers and 12 operators of root servers, including for instance Verisign (which operates two root servers) and RIPE NCC.
  - **Top-level servers** are authoritative servers for top-level domains (e.g. ".com" or ".fr"). They answer queries for records in their specific TLD and return addresses for authoritative name servers for second-level domains (SLDs). Top-level servers correspond to "registries" in the registration process.
  - **Second-level servers** are authoritative servers for second-level domains (e.g. "xyz.com" or "xyz.fr"). They answer queries for records in their specific SLD and return addresses for authoritative name servers for levels below, if appropriate. Second-level servers correspond to the DNS servers chosen by the registrant in the registration process.
- The **resolvers** (also referred to as recursive DNS servers) receive queries from the user application and query the authoritative servers to resolve the domain name into an IP address, as detailed above. They can be described as the "middle-man" between the user application and the authoritative servers. Any organisation or individual can set up their own resolver. Historically, the

resolver function has been operated by Internet Service Providers (ISPs). However, since the 2000s, open public resolvers have been increasingly used instead of the ISPs' own resolvers, as discussed below. Open public resolvers include Google (8.8.8.8), Cloudfare (1.1.1.1) and Quad9 (9.9.9.9).

- The **user application** (or "**client**", as opposed to "server") uses the DNS to access content (e.g. a website) or services. To access the desired content or service, the user application needs to query a resolver that will translate the domain name into information that will allow the client to connect to the named service, such as an IP address that corresponds to the host (see below).
- The **user** may be an individual or a machine (e.g., M2M).

For the registration process

The registration process enables an individual or an organisation (or "registrant") to lease a domain name through a registrar (or "seller"). The registrar then registers the domain name within a registry, which manages a TLD. To put content or services online, the registrant typically uses hosting service providers (e.g. web hosting).

- **Registries** are the organisations that manage TLDs. As of October 2021, there are **1589 TLDs** in the DNS (IANA, 2021[14]). However, there are less TLD operators, as some operate several TLDs. Amongst those, two main categories[6] can be distinguished:
  - Generic TLDs (gTLDs), which can be made of three-letter codes (e.g., ".com") or more (e.g. ".travel"), and are not bound to a specific country or territory. Most TLDs are gTLDs. Registries for gTLDs are designated by ICANN through Registry Agreements (RAs). ICANN develops policies for gTLD registries, which are enforced through the RAs.
  - Country-code TLDs (ccTLDs), which can only be made of two-letter codes corresponding to countries and territories, such as ".se" for Sweden or ".no" for Norway. As of October 2021, there are 316 ccTLDs amongst the 1589 TLDs. Most ccTLDs do not have an agreement with ICANN, and the governance of ccTLDs relies on the principle of subsidiarity. In fact, ccTLD policy issues are typically addressed by the local Internet community, and policies are set locally, according to applicable law[7] (GAC, 2005[15]; ICANN, n.d.[16]).
- **Registrars** are the organisations that sell a right-of-use of domain names directly to the registrant (gTLD registries are not allowed to do so, due to their registry agreements with ICANN). Registrars that serve gTLDs are accredited by ICANN through Registrar Accreditation Agreements (RAAs), while registrars selling domain names under ccTLDs enter into agreements with the relevant ccTLD registries. Registrars usually provide DNS host functions, i.e. services to manage the configuration that points the domain name to the corresponding IP address. There are around 2500 registrars accredited by ICANN, of which 20 hold a significant market share, e.g. GoDaddy.
- **Resellers** of domain names, which contract with registrars to sell a right-of-use of domain names to registrants. Resellers do not have a direct contractual relationship with ICANN.
- **Registrants** are the individuals or organisations that lease a domain name. This lease is bound by contractual arrangements between the registrant and the registrar, and typically lasts for a definite period (e.g. a year), and therefore has to be renewed regularly. Some ccTLDs allow registrants to lease domain names directly from the registry.
- While not part of the DNS strictly speaking (as outlined in Figure 1), content and services **hosts**[8] (also known as hosting providers, including web-hosting organisations) are key actors as they provide storage for and access to (through an IP address) the content and services for which the DNS ultimately functions.

Both registries and registrars are very diverse in terms of size, activities, governance structure, location and applicable jurisdiction. In addition, one organisation may perform several of the functions identified above (e.g. a registrar may also be a content host).

The role of ICANN

As outlined above, the Internet Corporation for Assigned Names and Numbers (ICANN) is often mistaken as the "global regulator" of the DNS and of website content. In reality, ICANN only co-ordinates some key aspects of the technical management of the DNS, including those aspects that require some degree of centralisation. For instance, ICANN operates the IANA, develops policies for and manages the assignment of gTLD registries, and accreditates gTLD registrars. ICANN also provides a platform for the multi-stakeholder community to meet and find common solutions to issues affecting the DNS, including regarding DNS security. Within ICANN, two advisory committees in particular provide advice regarding DNS security: the Security and Stability Advisory Committee (SSAC) and the Governmental Advisory Committee (GAC). Importantly, regulating website content is not part of ICANN's mandate[9].

Since its foundation in 1998, ICANN has developed policies through processes that are led by the multi-stakeholder community. Regarding gTLDs, these policies are enforced through contractual agreements: the RAs for gTLD registries and RAAs for gTLD registrars. The contractual power of ICANN can be leveraged by the multi-stakeholder community to refine and incentivise the use of best practices for DNS security. More recently, in the wake of high-profile digital security incidents that affected the DNS, such as DNSpionage and Sea Turtle, ICANN also decided to launch or reinforce multi-stakeholder initiatives specifically dedicated to enhancing DNS security, as outlined in Box 1.

Box 1. ICANN's initiatives to enhance DNS security

As a global platform that enables the multi-stakeholder community to collaborate and find innovative solutions to enhance the security and resilience of the DNS, ICANN has launched several initiatives that address key issues in this area:

DSFI-TSG

The DNS Security Facilitation Initiative Technical Study Group (DSFI-TSG) was launched in May 2020 to explore new ideas on what ICANN could and should do to increase the level of collaboration and engagement within the DNS ecosystem to improve DNS security. The group presented its recommendations to ICANN's CEO in October 2021, including the following:

- Examine the feasibility of funding DNS-related bug bounty programs;
- Raise awareness through educational programs about authentication best practices, registry lock, infrastructure security and DNS blocking and filtering;
- Encourage the deployment of a formalized incident response process across the DNS industry.

ITHI

The Identifier Health Technology Indicators (ITHI) is a project launched in 2016 by ICANN's Office of the Chief Technical Officer (OCTO). The goal of ITHI is to define metrics, perform measurements and assess trends over time relating to the "health" of the Internet's identifier systems, which includes but is not limited to DNS security. For instance, the project developed indicators in areas such as resolver integrity, DNSSEC deployment, resolver concentration and DNS abuse. For the latter, the metrics gathered through ITHI showed that in 2020 only one gTLD accounted for 50% of "phishing" instances and for 50% of "malware" instances, two categories of DNS technical abuse (ICANN, 2020[17]).

DAAR

The Domain Abuse Activity Reporting (DAAR) project is a system designed for studying and reporting on domain name registration and security threats across TLD registries. It offers a robust and reliable methodology for analysing security threat activity that the ICANN community can use to make informed policy decisions. The system collects TLD zone data and complements it with a large set of high-confidence Reputation Block List (RBL), i.e. lists of domain names and/or IP addresses that have been investigated and subsequently identified as posing security threats (e.g. phishing or malware).

The data collected by the system is used to generate DAAR monthly reports. The reports provide a monthly analysis of all TLDs for which data was available. They also provide aggregated statistics and time-series analyses about security threats such as phishing, malware, spam, and botnet command and control (ICANN, 2021[18]).

KINDNS

The Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDS) is a program launched in 2021 in the ICANN community. Its goal is to enable the sharing of concrete DNS security best practices and to build "soft consensus" around them. KINDNS also intends to develop a set of mutually agreed norms that could support a more secure DNS ecosystem, following the model of "MANRS" for routing security (see (OECD, Forthcoming[19])).

Source: ICANN

3. A tentative taxonomy for DNS security and DNS abuse

There is no internationally agreed definition of what DNS security precisely covers. Often, there is confusion between DNS security and DNS abuse, and these two categories may sometimes overlap. This section intends to provide a taxonomy to distinguish them. In the context of this report:

- **DNS security** relates to incidents that affect the availability, integrity or confidentiality of parts of the DNS ecosystem.
- **DNS abuse** is a broader category that includes any use of the DNS for malicious purposes, without necessarily resulting in a technical impact on the DNS itself.

As stated above, this report focuses on DNS security, as the scope entailed by DNS abuse would be much broader that what this report intends to cover.

DNS security

In the context of this report, DNS security is defined as the specific area of digital security that covers incidents disrupting the availability, integrity and confidentiality ("AIC triad") of parts of the DNS ecosystem. These incidents may impact any DNS actor, as well as any relationship between DNS actors (see Figure 1), through one or more of the following dimensions:

- **Availability**: part of the DNS ecosystem is not accessible and usable on demand by authorised users (e.g. a second-level authoritative server is no longer able to provide answers to a DNS query, because of a DNS flood attack (Imperva, n.d.[20])).[10]
- **Integrity**: part of the DNS ecosystem has been altered in an unauthorised manner (e.g. an organisation's domain name no longer points to the correct IP address because of a DNS hijacking attack).

- **Confidentiality**: part of the DNS ecosystem has been accessed by unauthorised entities (e.g. unencrypted DNS queries can be inspected by third parties, which may negatively impact user privacy, see (IETF, 2021[11])).

The key vulnerabilities of the DNS ecosystem, as well as existing efforts and emerging solutions to address them, are further discussed in section 4 and 5 below.

DNS abuse

There is no internationally agreed definition of "DNS abuse". Some stakeholders have adopted a broad definition of DNS abuse, which would include any illegal or abusive website content on the Internet within its scope. Others have adopted a more narrow definition, which limits DNS abuse to the categories of malware, botnets, phishing, pharming, and spam, when it serves as a delivery mechanism for the other four forms of DNS abuse[11] (DNS abuse framework, 2020[21]). A report recently developed within the ICANN multi-stakeholder community considers that DNS abuse can be defined as the "intentional misuse" of domain names "for cybercrime infrastructure" and to direct users to "websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud" (SSR2, 2021[22]).

In the context of this report, and to distinguish it from DNS security, DNS abuse refers to the use of the DNS for malicious purposes, without necessarily resulting in a technical impact on the DNS itself.

Therefore, what is often labelled as "addressing DNS abuse" should rather be understood as "DNS level action to address abuses online", i.e. leveraging the DNS ecosystem to solve issues that neither affect nor are caused by the DNS specifically (I&J, 2021[12]). In fact, most forms of DNS abuse relate to content and services that belong to the "content layer" outlined in Figure 1.

DNS abuse may encompass two categories:

- **The use of the DNS in digital security attacks**, impacting the AIC triad of Internet users, without any impact on the DNS itself. Domain names are typically an integral part of phishing campaigns and can be used by malware or for the Command and Control (C2 or C&C) platforms of botnets, i.e. the sets of tools that malicious actors use to communicate with compromised devices. The DNS can also be used as a "covert channel" to allow malicious traffic to flow unnoticed through "DNS tunnelling", which may also be used for data exfiltration. This category is often referred to as DNS "technical abuse" (I&J, 2021[12]), and may be considered as overlapping with DNS security.
- **The use of the DNS for illegal activities**, apart from digital security attacks, i.e. without any impact at the technical level on the AIC triad of Internet users or parts of the DNS, including the use of domain names to provide access to illegal content (e.g. copyrights infringements, hate speech, violent and extremist content, etc.). This category is often referred to as DNS "content abuse" (I&J, 2021[12]).

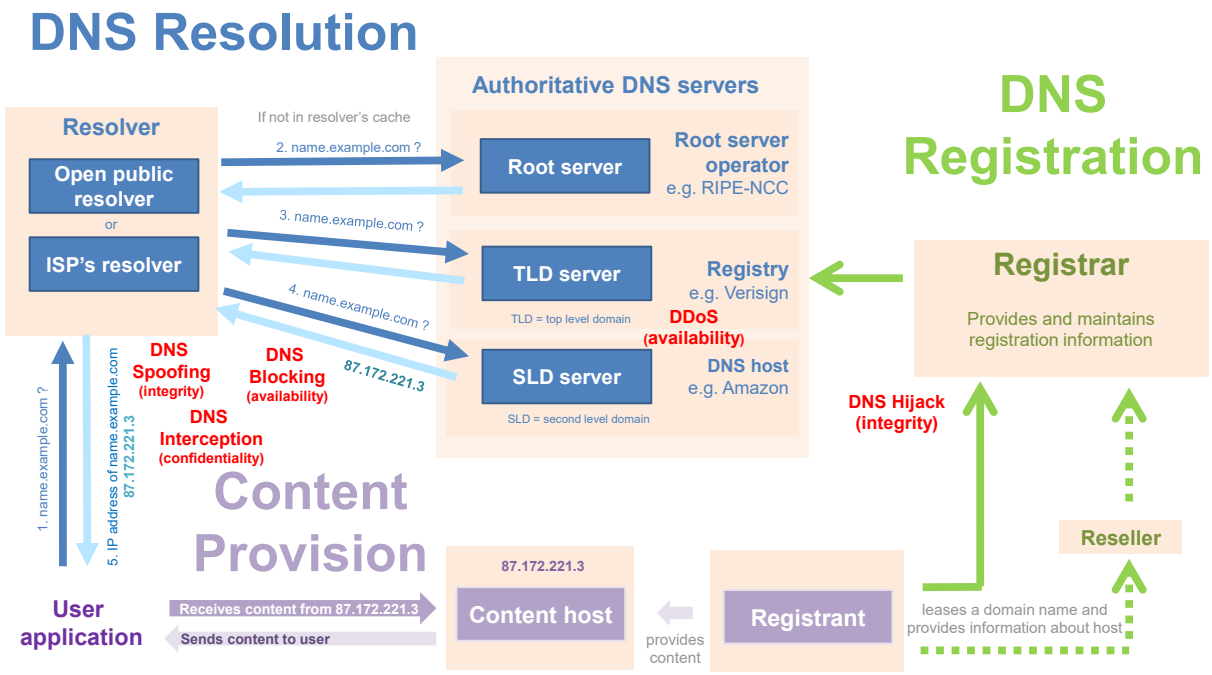
Current challenges and opportunities regarding DNS abuse are further discussed in Annex B.

4. Key vulnerabilities in the DNS ecosystem

As discussed above, DNS security covers incidents that may affect the availability, integrity and confidentiality of parts of the DNS ecosystem. Digital security incidents may result from the exploitation of vulnerabilities at any step of the resolution and registration processes described in Figure 1.

Figure 3 provides a few examples of such incidents. However, it does not intend to be exhaustive. In fact, any actor of the DNS ecosystem, and any relationship between those actors, may be subject to a digital security incident that could impact availability (e.g. blocking), integrity (e.g. spoofing or hijacking) or confidentiality (e.g. intercepting). An incident impacting content provision (e.g. a Distributed-Denial-of-Service or DDoS attack on the content host) would not be considered as a DNS security incident *per se*, because the content host (e.g. a web-hosting provider) does not belong to the DNS ecosystem understood in a narrow definition (logical layer).

Figure 3. Overview of potential incidents affecting DNS security



Note: This high-level overview does not intend to be exhaustive, but rather to provide a simplified picture of potential incidents in the DNS ecosystem. In fact, every relationship between DNS actors (represented by an arrow) can be subject to digital security incidents.
Dotted lines represent alternative or optional paths.
Source: OECD

With this context in mind, this section looks in particular at three types of vulnerabilities whose exploitation may affect the availability, integrity or confidentiality of the DNS ecosystem:

- **"DNS-specific" vulnerabilities**, which result from flaws in the DNS protocol and its implementation (IETF, 2004[23]). These include, for instance, a lack of mechanisms to control the integrity and confidentiality of DNS traffic, allowing unauthorised third parties to forge responses and redirect users to malicious websites, or allowing them to intercept DNS queries.
- **Vulnerabilities of DNS actors**, which may result from code vulnerabilities in the software used by these actors, misconfigurations, insufficient access controls (e.g. lack of a robust multi-factor authentication mechanism for a registrant's account in the registrar's platform) and the human

factor (e.g. social engineering). They also include supply-chain attacks that would compromise registrars or resellers to reach their ultimate targets.

- **Dependencies and emerging concentration in the DNS ecosystem**, which could have significant consequences for DNS security (e.g. single points of failure with the risk of cascading effects).

"DNS–specific" vulnerabilities

Originally, the DNS protocol and the ecosystem implementing it were designed as a public database with little security controls regarding confidentiality and integrity, as the Internet was not intended to be used by the general public (ICANN, 2019[5]). [12] In fact, the design of the DNS ecosystem focused on ensuring the availability and efficiency of domain name resolution. Since the Internet has expanded in the 1990s and has become increasingly critical to the functioning of the economy and society, the multi-stakeholder community has worked together to develop new approaches to DNS security and implement more effective security measures (e.g. extensions of the DNS protocol). Nevertheless, the DNS ecosystem contains many vulnerabilities related to the DNS protocol itself, to flaws in its implementation, or to the way the DNS is structured (DSFI-TSG, 2021[24]).

To disrupt the functioning of the DNS ecosystem, malicious actors may seek to exploit vulnerabilities in the DNS protocol resulting in breaches of i) confidentiality, ii) integrity and iii) availability.

Confidentiality

Historically, the DNS resolution process has relied on unencrypted packets, i.e. transport in clear text. The use of unencrypted packets enables almost anyone, including malicious actors, to observe, collect, process and transfer data relating to DNS traffic (IETF, 2013[25]). DNS query data may be monitored and stored for commercial and marketing purposes, as well as for governmental surveillance purposes.

The lack of confidentiality of DNS traffic may significantly impact user privacy, as some DNS queries may reveal sensitive personal data such as religious beliefs, political opinions or health conditions (IETF, 2021[11]). It may also raise social concerns in the case of large-scale population monitoring by governments or corporations. Such vulnerabilities may also be exploited by malicious actors to to carry out digital security attacks (e.g. as they provide technical information about organisations' devices and applications and real-time information about users' near-term future service transactions).

Integrity

Historically, integrity was not a major consideration for the design of the DNS protocol and of the ecosystem implementing this protocol. DNS responses traditionally do not have a cryptographic signature, enabling malicious actors to spoof responses at various stages of the DNS resolution chain, i.e. to intercept and respond to DNS queries with incorrect data (Wei and Heidemann, 2011[26]).

Integrity attacks leveraging flaws in the DNS protocol typically rely on the impersonation of resolvers or authoritative servers by malicious actors (DSFI-TSG, 2021[24]). Malicious actors can easily impersonate authoritative servers when no digital signature is used to validate DNS data. Such impersonation enables DNS redirection, i.e. when domain names are incorrectly resolved and redirect users to malicious websites. Impersonation can leverage look-alike domains (Facsimile domains), e.g. through domain suffix appending (e.g. www.oecd.org.example.com instead of www.oecd.org), typosquatting (e.g. oedc.org instead of oecd.org) and internationalized domain name homographs (e.g. oécd.org instead of oecd.org) (DSFI-TSG, 2021[27]).

Even though their effects may lead to the same consequences (e.g. DNS redirection), impersonating actors of the resolution process should not be confused with changing DNS configuration by attacking actors of

the registration process. The former usually relies on the interception of traffic at the network layer, while the latter results from the exploitation of vulnerabilities (e.g. code vulnerabilities, misconfigurations, social engineering) of a registrant, a registrar or a registry (see below) that enables a change in DNS configuration.

Impersonation of DNS actors can be done through DNS spoofing and DNS cache poisoning, i.e. when malicious actors insert incorrect data into a resolver's cache (DSFI-TSG, 2021[27]). Poisoning can occur when an on-path malicious actor intercepts a query and generates its own response, or when an off-path attacker is able to successfully spoof a response that appears to come from a legitimate responder. The incorrect data may remain in the cache for an amount of time determined by the Time-To-Live (TTL) values, the amount of time during which a resolver stores resolution information in their cache memory (DSFI-TSG, 2021[27]). Examples of attacks leveraging such vulnerabilities include Dan Kaminsky's cache poisoning attack (DSFI-TSG, 2021[24]) and GhostDNS, a platform developed to help attackers find vulnerable routers and change the DNS settings of those that are exploitable. Most notably, attackers have used GhostDNS to target Brazilian financial institutions and their customers (Hopkins and Byers, 2020[28]).

Malicious actors may also leverage the expiry date of domain names' lease to carry out attacks. In fact, expired or cancelled domain name registrations allow malicious actors to lease domain names that formerly pointed to legitimate websites, and to redirect users towards malicious ones. Another attack vector includes the use of the "lost credentials" function in the platform of certain registrars. These attack vectors are all the more successful when protection measures such as registry locks or multi-factor authentication are not implemented by actors of the registration process (see below).

Availability

Historically, availability was a key concern in the design of the DNS ecosystem. As a result, the DNS as a whole is often considered as relatively robust and resilient to availability attacks because of built-in redundancy mechanisms.

However, actors of the DNS ecosystem are vulnerable to distributed-denial-of-service (DDoS) attacks, i.e. attacks that breach the availability of a target by flooding it with a large number of requests, hence preventing legitimate users to access it during a few minutes or for entire days. For instance, there have been cases of malicious actors launching DDoS attacks on the ccTLD registries of the People's Republic of China (".cn") in 2013 (Mimoso[29]) and Türkiye (".tr") in 2015 (Sozeri[30]), resulting in the unavailability of moderate access issues for SLDs under each TLD. In 2016, malicious actors used the Mirai botnet to launch a DDoS attack on DNS service provider Dyn, which disrupted the operations of major companies such as Twitter and Amazon for a few hours (OECD, 2021[31]). Such DDoS attacks demonstrate the criticality of the DNS ecosystem as well as the interdependence of DNS actors.

One may argue that there may be some overlap in this case between "DNS-specific" vulnerabilities and vulnerabilities of DNS actors, as DDoS attacks are not specific to the DNS and could target other actors such as web-hosting providers. However, an important aspect of DDoS attacks that target DNS actors is that their impact is maximised because of the hierarchical structure of the DNS. For instance, making a TLD registry unavailable is likely to impact all SLDs below that TLD (at least in case resolvers do not have the relevant resolution data in cache). In that regard, such vulnerabilities may be considered "DNS-specific" as they result from the hierarchical structure of the DNS. However, the effective and secure use of caching by resolvers enables stakeholders to mitigate this specific risk.

In addition, DNS-based DDoS attacks have an amplification effect because DNS responses are usually larger (and sometimes many times larger) than the corresponding DNS queries (DSFI-TSG, 2021[24]). These reflective amplification attacks are DDoS attacks in which malicious actors use publicly accessible, open recursive resolvers to flood a target system with DNS response traffic. In that case, the use of DNSSEC signature aggravates the amplification effect, as responses and queries involving DNSSEC signature or validation are typically larger (see below). Recent research showed that in 2021 there are up

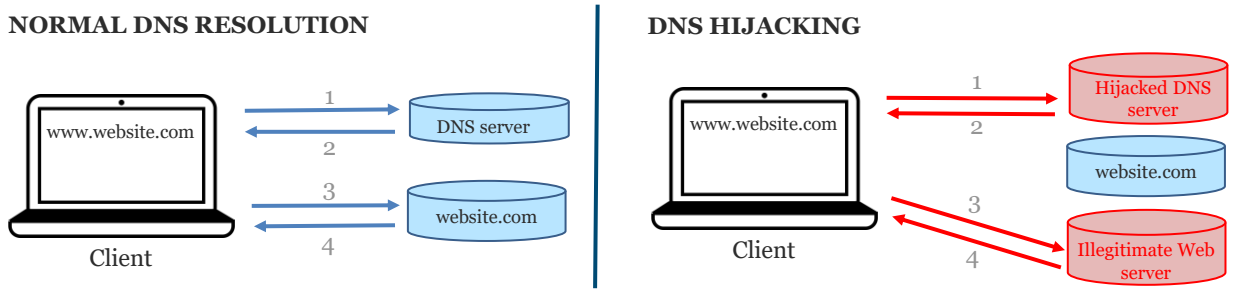
to 6 million open resolvers that can be used to amplify DDoS attacks, the vast majority of which being inadvertently open due to misconfigurations (Huston, 2021[32]).

Vulnerabilities of DNS actors

Digital security incidents affecting the DNS may also result from the exploitation of vulnerabilities of DNS actors, such as lack of access controls, code vulnerabilities, misconfigurations or theft of credentials, e.g. through social engineering. These vulnerabilities are not "DNS-specific" in that they do not result from flaws in the DNS protocol or its implementation.

The exploitation of such vulnerabilities in actors of the DNS registration process (i.e. registrants, resellers, registrars and registries, see Figure 1) may enable DNS hijacking (see Figure 3), i.e. when malicious actors modify DNS configuration to incorrectly resolve domain names in order to redirect users to malicious websites (DSFI-TSG, 2021[27]). Figure 4 illustrates the effects of a DNS hijacking.

Figure 4. Effects of DNS hijacking



Source: OECD

Such attack can be performed through social engineering or malware targeting the direct victim itself (i.e. the registrant), enabling malicious actors to steal the credentials used by the registrant to manage their DNS configuration (e.g. through the registrar's platform). For instance, in 2018, malicious actors targeted the DNS ecosystem in Middle-Eastern countries such as Lebanon and the United Arab Emirates (UAE). In this attack, referred to as "DNSpionage" and attributed to a state-sponsored actor, or Advanced Persistent Threat (APT), the attackers infected their victims' networks and retrieved DNS credentials (the information used by the registrant to access the management interface for their domain names). Then, they hijacked the targets' domain names and redirected traffic from the legitimate domain names to IP addresses they controlled. Victims included the Lebanese Ministry of finance and an airline company, amongst others (Cisco, 2018[6]).

Another way to modify DNS records is by attacking the ''DNS registration supply chain'', e.g. a registrar or registry. The relative complexity of the DNS registration supply chain described above (registry, registrar, reseller, registrant, hosts and other DNS providers) provides many opportunities for malicious actors. In recent years, there have been many cases of supply-chain attacks targeting DNS actors. For instance, malicious actors have targeted registrars such as Gandi and GoDaddy to steal their clients' credentials or gain access to their clients' IT systems. In 2015, "Lenovo.com" was hijacked following an attack on "webnic.cc", a Malaysian registrar (Krebs, 2015[33]). In 2019, the Sea Turtle hijacking saw Armenia's ".am" top-level domain compromised, amongst others. In this attack, the targets were infected through spearphishing emails and hacking tools designed to exploit code vulnerabilities. Once the malicious actors gained full access to a registrar or registry, they changed the final target organization's domain registration to point to IP addresses under their control, instead of the victim's legitimate ones. When users then

attempted to reach the victim's network, malicious actors would harvest usernames and passwords from the intercepted traffic (Wired, 2019[7]).

Dependencies and emerging concentration in the DNS ecosystem

As mentioned above, the DNS ecosystem overall is largely and globally distributed. However, some stakeholders have raised concerns in recent years regarding certain dependencies and emerging patterns of concentration at some levels of the DNS ecosystem.

The impact of digital security incidents affecting the DNS ecosystem may significantly increase in case of dependencies or if there is a higher level of concentration in parts of this ecosystem. In fact, dependencies and increased concentration could result in the emergence of single points of failure, whose disruption could have significant cascading effects. From a digital security perspective, dependencies and increased concentration represent a vulnerability that elevates the risk level, as successful attacks on a single or a few providers could have adverse consequences on the entire ecosystem.

Beforehand, it is important to note that concentration is not an issue specific to the DNS, as it rather affects the digital ecosystem as a whole (ISOC, 2019[34]). In recent years, many facets of the digital economy have moved from entrepreneurial ventures to established business practices, resulting in amalgamation and market concentration (Huston, 2021[32]). Second, the topic of concentration cannot be examined solely through the lens of security, as it impacts many other policy areas such as privacy, competition, consumer protection, innovation or strategic autonomy. This report, however, only intends to examine DNS security, and its relationship with concentration within the DNS ecosystem.

This section looks in particular at i) supply-chain dependencies in the DNS ecosystem and ii) emerging concentration at the level of DNS resolvers.

Other areas where concentration may raise concerns include hosts and authoritative servers. However, as outlined in Figure 1, content hosts (i.e. web-hosting services) should be considered as outside the DNS ecosystem strictly speaking. Regarding authoritative servers, as of February 2022, there are more than 2500 gTLD registrars and more than 1580 TLDs (see above), the majority of which having been delegated following the round of applications for new gTLDs launched by ICANN in 2012. As a result, experts usually agree that key security concerns in this area relate to the digital security risk management practices of these actors (or lack thereof) rather than to their concentration. Finally, regarding the 12 root server operators, their relative concentration does not appear to raise specific concerns regarding DNS security, for reasons more detailed below, and putting aside geopolitical concerns, which are out of scope of this report.

Supply-chain dependencies in the DNS ecosystem

Single points of failure for the DNS ecosystem may not only result from concentration at the level of the main DNS actors described in Figure 1. They could emerge from a small actor of the DNS supply chain, such as a DNS service provider or a software supplier.

Regarding communication networks more generally, dependencies are often associated with a lack of competition and innovation at certain layers of the supply chain, resulting for instance from barriers to entry or from a lack of economic interest in developing certain niche markets. A lack of diversity in the supply chain may result in a high degree of reliance on a single supplier and make it more difficult to procure solutions from other suppliers, especially where solutions are not fully interoperable. In fact, supply-chain dependencies often lead to closed technical “monocultures” that are prone to systemic risk, as they increase the likelihood that a single vulnerability creates a widespread outage simultaneously affecting many actors.

Regarding DNS security in particular, an early concern was the lack of diversity of implementations of the protocol standards (Huston, 2022[35]). In particular, stakeholders identified in the 2000s a single point of failure in Berkeley Internet Name Domain (BIND), a DNS management software that was used by most if not all the main actors of the DNS ecosystem, including root servers (Afilias, 2009[36]). As a result, the exploitation of a single code vulnerability in BIND could have had systemic consequences on the entire DNS ecosystem.

However, this specific concern regarding DNS management software has since been addressed by the multi-stakeholder community, which diversified the supply chain by developing alternative, open-source solutions, as discussed below.

DNS resolvers

As discussed above, DNS resolvers can be described as the "middle-man" between users (or clients) willing to access content through the DNS on one hand, and authoritative servers (which provide the information necessary to connect to a named service, e.g. to resolve the domain name into the correct IP address) on the other hand. Resolvers are a key pillar of the DNS ecosystem.

Any organisation or individual can set up their own resolver, subject to available resources and technical know-how. However, historically, the function of resolver has been bundled with other services provided by ISPs: until the 2010s, the vast majority of DNS queries was resolved by ISPs' own resolvers (Huston, 2021[32]).

Since the 2010s, there has been a change in the landscape of the resolver market, with the development at scale of open public resolvers, i.e. resolvers that accept DNS queries from all IP addresses, contrary to ISPs' resolvers which normally only accept queries from their own networks (Huston, 2019[37]). Google started[13] to provide such services in 2009, followed by Quad9 (2016) and Cloudfare (2018) (Radu and Hausding, 2020[38]). [14]

Available data and analysis

There is no internationally agreed methodology to precisely and objectively measure the concentration of the resolver market. As there is no financial transaction (users do not pay for DNS resolution), measurements typically examine the number of queries that are performed by visible resolvers. Recent analysis and studies usually reach the same overall conclusion: there has been, since the 2010s, an increasing reliance of Internet users on open public resolvers, and in particular on Google's open resolver (Radu and Hausding, 2020[38]; Huston, 2021[32]). According to recent estimates, Google's resolver accounts for between 15% and 30% of the resolver market (depending on the measurement methodology, e.g. taking into account their role as back-up resolvers), while ISPs taken altogether account for around 70%[15] of the market. According to this study, other open resolvers such as Cloudfare and Quad9 account for respectively 3% and 1% market shares.[16] Another study, based on a different methodology, suggests a higher market share for Cloudfare, around 13% (Radu and Hausding, 2020[38]). In both cases, this movement represents a significant shift from how the market was structured before the 2010s, where it would typically take 10 ISPs to serve 30% of Internet users (Huston, 2021[32]).

Available data therefore suggests there is a clear trend towards concentration of the resolver market, resulting in particular in the increasing reliance of Internet users on Google's resolution service. While some have observed a relative stabilisation of market shares for open public resolvers in the past two years (ICANN, 2021[39]), other experts consider that Google's market share in the resolver market is likely to continue to grow.

In that regard, another trend that raises significant concerns in the DNS multi-stakeholder community is that the choice of the DNS resolver is increasingly embedded at the level of the application, as opposed to being made by the ISP or the user (SSAC, 2020[40]). With Google's Chrome holding a 65% market share

for browsers (Statista, 2021[41]) and Google's Android a 72% market share for mobile devices' operating systems (Statcounter, 2021[42]), this trend is likely to further increase resolver concentration towards Google's open resolver.

This switch to open public resolvers may be the result of a decision made by an individual user, an organisation's network manager, or by the ISPs themselves. The decision to switch to an open resolver is usually motivated by technical performance and reliability. For instance, following the outage of an ISP's resolver, users would switch to an open public resolver and continue using it afterwards (Radu and Hausding, 2020[38]). Another important motivation for switching to open resolvers is the willingness to circumvent DNS blocking established at the ISP level. ISPs typically implement DNS blocking to comply with national law, including judiciary decisions or administrative requests (e.g. blocking the resolution of certain names considered to be associated with various forms of DNS abuse, see below). In fact, if open resolvers are not located in the user's country, they would typically not be subject to national law[17]. Open public resolvers such as Google, Quad9 and Cloudfare also usually provide best-in-class security measures, for instance by enabling DNSSEC validation and encrypted DNS transport (e.g. DoH / DoT, see below), whereas some ISPs' resolvers do not offer the same level of protection.

Impact on DNS security

Overall, users and ISPs may switch to open resolvers because of the enhanced security that they can provide. In fact, the switch to open resolvers can provide, or be perceived as providing:

- Enhanced availability, i.e. less likelihood of outages.
- Enhanced integrity, through DNSSEC validation and DNS blocking measures limited to cybersecurity risk (e.g. malicious domains used to spread malware), as opposed to DNS blocking measures focusing on content such as copyrights infringements.
- Enhanced confidentiality, through the use of encrypted DNS transport techniques (e.g. DoH and DoT), which prevent ISPs and other entities to intercept the user's DNS queries.

However, rather than eliminating DNS digital security risk entirely, users that switch to open resolvers mitigate some aspects of the risk while exposing themselves to other aspects. For instance, in the case of Google's open public resolver (which provides encrypted DNS transport), confidentiality is in fact enhanced as no other entities than the user and the resolver are able to access the data associated with the DNS queries. With a typical ISP resolver that does not provide DNS transport encryption, there would be no confidentiality for this data. However, from another perspective, the resolver continues to benefit from a full access to the data associated with the DNS queries, and there may be limited safeguards regarding the application of national privacy laws (e.g. in the European Union, the General Data Protection Regulation or GDPR) if the resolver processes data in other jurisdictions, and in the absence of an adequacy decision. Privacy concerns regarding the impact of Google's resolver increasing market share are reinforced by the fact that there is no financial transaction associated with DNS resolution, and little transparency on how Google processes the data associated with DNS queries (Huston, 2021[32]). In other words, a possible way for a for-profit resolver to have a financial interest in providing this "free" service is to exploit the data associated with the user's DNS queries. The increasing market share of Google's resolver therefore raises legitimate concerns regarding the confidentiality dimension of DNS security. More broadly, the concentration of exchanges (DNS queries and responses) towards a small number of actors could be considered as an emerging systemic risk, as it would allow massive population monitoring.

The increasing concentration of the resolver market also raises questions regarding DNS integrity. Theoretically, a dominant market player in the resolver market could unilaterally decide to stop resolving a domain name, or an entire TLD, which would considerably impact the integrity of the DNS (Huston, 2019[37]). Such integrity breach by an ISP's resolver would be limited to a much less significant market share. Similarly, an availability incident affecting Google's resolver could impact a significant portion of Internet users and have considerable cascading effects (i.e. a form of systemic risk).

On the other hand, some experts consider that these risks are limited by the fact that there are little barriers to entry and little switching costs in the resolver market, and that such incidents would be visible enough to incentivise users to switch to other resolvers. However, as discussed above, the ability for users to switch resolvers could significantly decrease as the choice of a DNS resolver becomes increasingly embedded at the application level.

Root servers

As described above, root servers are the authoritative servers for the root zone. Historically, policy interest in the concentration of root servers has been mostly motivated by geopolitical considerations (which are out of the scope of this report), rather than by concerns relating to DNS security.

There are 13 root servers, which are operated by 12 different organizations (VeriSign operates two root servers), most of which being headquartered in North America:

- VeriSign ;
- University of Southern California, Information Sciences Institute ;
- Cogent Communications ;
- University of Maryland ;
- NASA Research Centre ;
- Internet Systems Consortium ;
- Department of Defense (DoD) Network Information Centre ;
- US Army Research Lab ;
- Netnod ;
- RIPE NCC ;
- ICANN ;
- WIDE Project.

However, while there are only 12 root name server operators, there are more than 1510 root server instances (as of February 2022), which are globally distributed (Netnod, 2020[43]; Root-servers.org, n.d.[44]; Packet Clearing House, 2021[45]). Such distribution and redundancy tend to limit the likelihood of a global unavailability of the DNS resulting from a digital security attack targeting root name servers. Because root servers are available from locations all around the world, the current model of distributed, redundant and independent operations contributes to enhance DNS availability (RIPE NCC, 2020[46]). In addition, the signing of the root zone with DNSSEC (see below) enables to ensure the integrity of root servers' responses to DNS queries.

The resilience of root servers has also been reinforced by the use of techniques such as Anycast, a network routing methodology that enables any instance (usually, the closest data centre) of any root server to provide correct responses to any query regarding the root. Resolvers use the average response time to select the DNS server that provides the fastest response, ensuring that the client always connects to the most "local" of the available instances. In case of a failure to respond, clients will automatically be diverted to a functioning alternative.

The efforts of the DNS multi-stakeholder community to ensure the resilience of the root servers have resulted in the absence of any significant incident affecting them in the last two decades. In 2002, an attack targeted all root servers and almost led to an outage of the DNS, but was unsuccessful in the end (Cornell, 2002[47]). This attack resulted, however, in efforts by the DNS multi-stakeholder community to increase resilience and contributed to the adoption of Anycast by root servers. In 2015, DDoS attacks targeting root servers also failed to impact the global availability of the DNS, confirming the robustness of the DNS ecosystem and the importance of Anycast design for critical infrastructure (Moura et al., 2016[48]).

Finally, the 12 root server operators adopted specific strategies to diversify their supply chain and enable organizational and technical autonomy. At the technical level, operators use different combinations of hardware and software to prevent the emergence of single points of failure, as discussed above in the case of BIND.

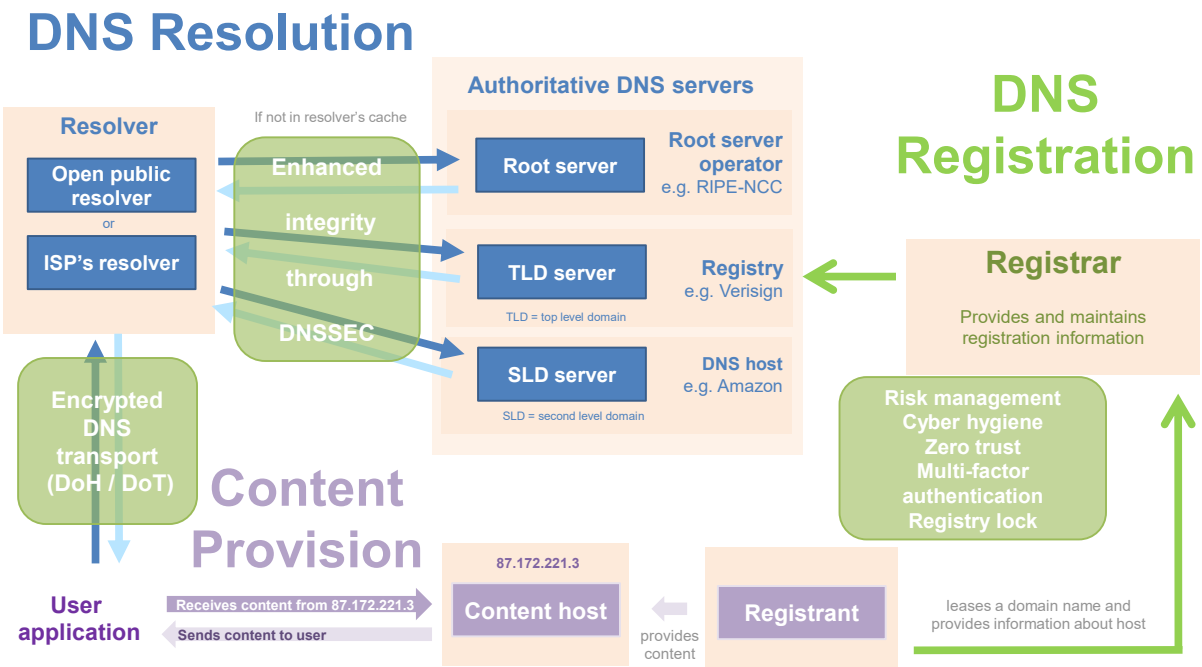
To conclude, root servers, and the hierarchical structure of the DNS more broadly, might be perceived as a vulnerability, as a breach of the availability or integrity of an entire level of the hierarchy would impact the resolution of all domain names below that level. However, the distributed structure of root server instances and the implementation of technical innovations such as Anycast and DNSSEC contribute to support DNS security at the root level. As such, root servers should therefore not be considered as a key security vulnerability for the DNS. However, given their criticality, there is a need for the multi-stakeholder community in charge of their operations to regularly monitor the threat landscape and ensure that their risk management frameworks are adapted.

5. Existing efforts and emerging solutions to enhance DNS security

This section provides an overview of existing efforts and emerging solutions (see Figure 5) to address the key vulnerabilities identified in the previous section. Importantly, this section highlights that there is no "silver bullet", i.e. a perfect solution that would address all the challenges previously identified and finally "secure" the DNS ecosystem. Given the highly complex, dynamic and distributed nature of the DNS ecosystem, addressing DNS security vulnerabilities require action at many levels, and builds upon many technical solutions and organisational best practices. In addition, as there is on-going research in the multi-stakeholder community to develop new techniques and approaches to enhance DNS security, a specific solution that may appear as promising now may be considered as outdated or ineffective in a few years from now.

Importantly, each "partial solution" outlined in Figure 5 addresses specific vulnerabilities, while potentially raising other challenges in other dimensions of DNS security. For instance, DNSSEC enhances the integrity of the data exchanged between authoritative servers and resolvers, but could also increase the likelihood of availability incidents, in particular if misconfigured, or through amplification attacks. In addition, DNSSEC does not enhance DNS confidentiality, or integrity at other levels of the DNS resolution and registration processes (e.g. between the resolver and the user, or between the registrant and the registrar). Similarly, encrypted DNS transport only enhances the confidentiality of the data exchanged between the user and the resolver, as ISPs and other entities would no longer have unimpeded access to this data. However, the resolver would still have full access to such data.

Figure 5. Overview of existing efforts and emerging solutions to enhance DNS security



Note: This high-level overview does not intend to be exhaustive.
Source: OECD

Addressing "DNS-specific" vulnerabilities

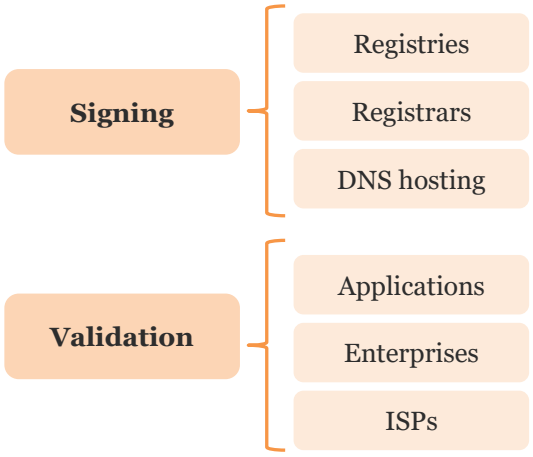
DNSSEC: enhancing data integrity between resolvers and authoritative servers

The Domain Name System Security Extensions (DNSSEC) are a suite of protocol extension specifications developed by the IETF that strengthens DNS security by enhancing the integrity of the data sent by authoritative servers to resolvers. DNSSEC enables authoritative servers to use digital signatures based on public key cryptography[18], hence allowing resolvers to detect forged or manipulated DNS responses. DNSSEC adds two important features that help strengthen the integrity of the DNS:

- Data origin validation, which allows the resolver to verify cryptographically that the data it received actually came from the zone where it believes the data originated.
- Data integrity protection, which allows the resolver to know that the data has not been modified in transit since the zone owner originally signed it with the zone's private key.

DNSSEC implementation therefore prevents certain types of attacks involving DNS spoofing (see above) between authoritative servers and resolvers. To be effective, DNSSEC deployment requires resolvers to validate DNSSEC on one hand, and authoritative servers to sign their zones with DNSSEC on the other hand (from the root level to TLDs, SLDs and below), as shown in Figure 6.

Figure 6. DNSSEC deployment requires both validation and signing



Source: Based on (Internet Society, 2014[49]).

However, DNSSEC deployment at the global level is not widespread yet, despite being available for more than a decade.

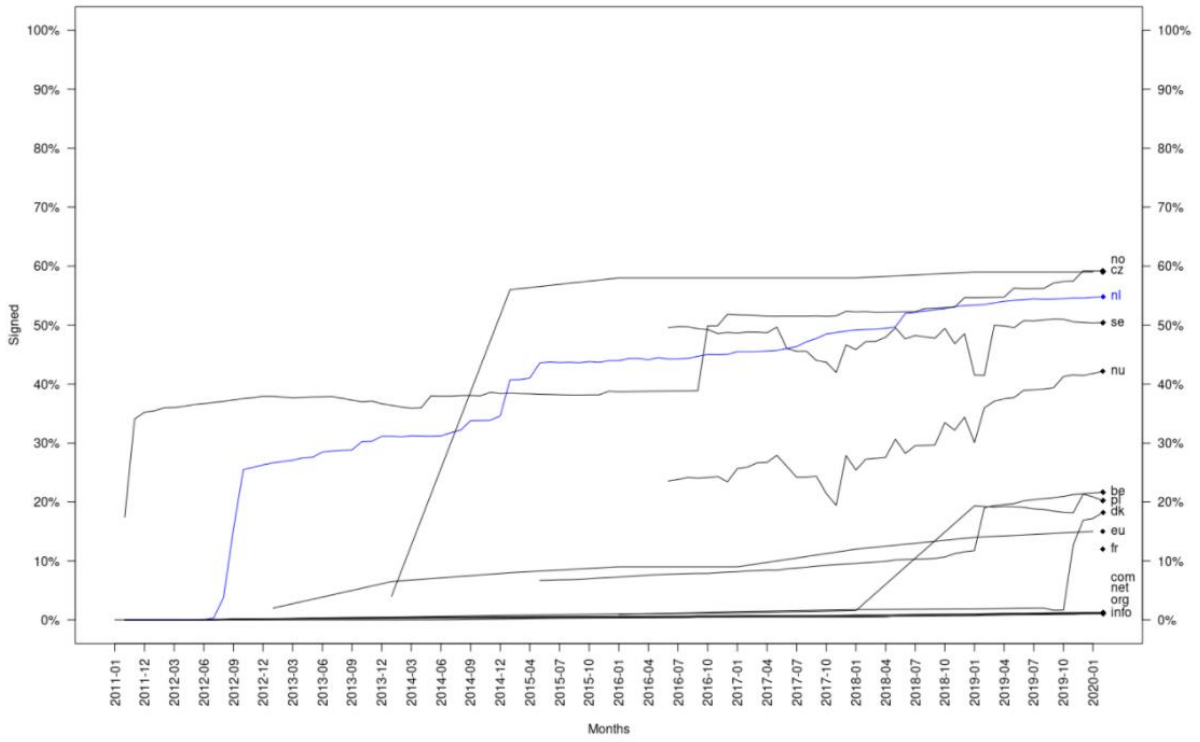
Regarding DNSSEC signing, all root servers and gTLDs have deployed it for their zones (ICANN, 2020[50]). However, it is not yet deployed in many gTLD subdomains and in some ccTLDs. There is no internationally agreed methodology to measure the adoption of DNSSEC signing below TLDs.[19] As a result, there is a lack of robust, internationally comparable data regarding DNSSEC signing. Nevertheless, some stakeholder-led efforts provide useful information, while somewhat subject to methodological biases.[20] For instance, StatDNS' estimates show that the rate of DNSSEC-signing for second-level domains may vary significantly, from below 3% for ".com" to above 30% for ".ch" and even higher for certain ccTLDs and brand TLDs (StatDNS, 2022[51]).

Regarding DNSSEC validation, estimates show that as of October 2021, around 37% of resolvers perform DNSSEC validation (ICANN, 2021[39]). The Asia-Pacific Network Information Centre (APNIC) regularly

publishes data on the rate of DNSSEC validation per country (APNIC, 2021[52]). These rates vary significantly across countries.

The significant gaps across countries in both validation and signing rates indicate the importance of stakeholder-led initiatives to incentivise the use of DNSSEC. In fact, stakeholders in countries such as Czechia, Finland, the Netherlands, Norway and Sweden have successfully developed initiatives to incentivise the use of DNSSEC, which resulted in significant increase of DNSSEC adoption, compared to other TLDs, as shown in Figure 7.

Figure 7. The key role of economic incentives to increase DNSSEC adoption



Note: this figure shows the significant increase of DNSSEC-signed second-level domains for ccTLDs where the registry launched schemes that provided financial incentives for registrars. They include the ccTLDs of countries such as Czechia, the Netherlands, Norway and Sweden, where the rate of DNSSEC-signed domains rose above 50%. For other TLDs where no similar schemes were launched, the rate stayed below 25%. The ccTLD ".nu" is operated by the Swedish ccTLD.
Source: (SIDN, 2020[53]).

These initiatives typically rely on schemes developed by the ccTLD registry to provide financial incentives to registrars and registrants for DNSSEC signing (SIDN, 2020[53]). Typically, the fee paid by the registrar to the registry for each domain would be lower for DNSSEC-signed domains. In Finland, the Transport and Communications Agency, Traficom, launched in 2019 a multi-stakeholder partnership with key DNS actors to further develop the use of DNSSEC, which culminated in a "national DNSSEC launch day" (Traficom, 2020[54]). With Traficom's initiative, the number of ".fi" registrars providing DNSSEC signing services increased from 10 in 2018 to more than 250 in 2020. These efforts resulted in the DNSSEC validation rate in Finland increasing from below 50% in 2018 to more than 80% in 2020. In Sweden, a similar success relied on a multi-stakeholder initiative, as discussed in Box 2.

Box 2. DNSSEC in Sweden: a success driven by the multi-stakeholder community

Sweden is one of the leading countries for the adoption of DNSSEC, as shown in Figure 7. This is the result of an effort led by the Swedish registry responsible for the ".se" TLD, the Swedish Internet Foundation (IIS), which was supported by the government of Sweden.

The IIS was the first registry in the world to sign its TLD with DNSSEC (2005) and to offer a complete DNSSEC service (2007). It then convinced important Swedish Internet users such as public authorities, banks, municipalities and counties to sign their subdomains with DNSSEC. The IIS also convinced the largest Swedish ISPs to turn on DNSSEC validation on their resolvers.

The Swedish Post and Telecommunications Agency contributed to financing, training and implementing the DNSSEC in municipalities' information systems. Out of 290 municipalities, 231 were granted a total of SEK 10 million (EUR 1 million) to introduce the DNSSEC in 2012-14. Private sector organisation Interlan offered a testing tool for municipalities to see on a map which DNSSEC implementation is active, works as expected or generates errors (see https://kommunermeddnssec.se). This tool generated a healthy competition between municipalities.

The number of signed domain names skyrocketed as of 2011 when the IIS offered registrars a yearly discount of SEK 6 for every correctly signed domain name in their portfolio.

The example of DNSSEC in Sweden shows how multi-stakeholder initiatives based on partnerships, education and economic incentives can deliver significant benefits for DNS security.

Source: (OECD, 2018[55])

Another benefit of DNSSEC is that it enables the use of DANE (DNS-based Authentication of Named Entities). Developed in the 2010s, DANE allows digital certificates to be bound to domain names using DNSSEC, instead of relying on certificate authorities. Digital certificates issued by certificate authorities are commonly used to provide encryption for Transport Layer Security (TLS), the security protocol that protects web (i.e. HTTP) and email transactions. With DANE, the administrator of a domain name can certify the cryptographic keys used in that domain by storing them in the DNS. However, DANE needs the DNS records to be signed with DNSSEC. In addition, DANE allows a stakeholder to specify which certificate authority is allowed to issue certificates for a particular resource, preventing another, potentially compromised certificate authority to issue a technically valid certificate for that domain.

Despite the important benefits it provides for DNS integrity, DNSSEC should not be perceived as a "silver bullet". DNSSEC should rather be considered as a key building block to enhance DNS security, which nevertheless faces certain limitations and challenges. In particular, DNSSEC:

- Enhances the integrity of the data exchanged between resolvers and authoritative servers, but does not enhance availability or confidentiality. Similarly, DNSSEC does not enhance integrity at other levels of the resolution and registration processes (e.g. between users and resolvers, or between registrants and registrars);
- Is a relatively complex protocol extension whose implementation is often considered as cumbersome (Rasmussen, 2010[56]);
- Significantly increases the size of DNS response packets, which make DNSSEC-aware DNS servers even more effective as DDoS amplifiers;
- Increases the resolver's workload, which may negatively impact technical performance (e.g. timeouts);

- Cannot be used as a market differentiator for end-users, as they are typically unaware that DNSSEC is used, which limits stakeholders' incentives to deploy DNSSEC.

The challenges outlined above may contribute to explain the relatively low adoption of DNSSEC at the global level, highlighting once again the complexity of addressing DNS security, as each solution comes with limitations as well as trade-offs with other objectives (e.g. technical performance, profitability, usability…) and with DNS security itself.

Encrypted DNS transport: enhancing DNS confidentiality between users and resolvers

To enhance DNS confidentiality, new technical standards have been developed to transport DNS queries and responses over alternative transport protocols[21] that encrypt data, examples of which are DNS over HTTPS (DoH) and DNS over TLS (DoT):

- DoH was introduced in Google's resolution service in 2016 and standardised by the IETF in 2018 (IETF, 2018[57]);
- DoT was standardised by the IETF in 2016, and the first organisations to implement DoT at a global scale were Google, Cloudflare and Quad9.

Such efforts move away from unencrypted UDP and TCP protocols (the traditional protocols used to transport DNS traffic), enabling the encryption of the data exchanged between users and resolvers. The use of encryption provides a certain level of confidentiality for the DNS queries and responses, in that a third party that spies on Internet traffic will not be able to determine their content. By encrypting plaintext DNS traffic, DoT and DoH prevent interception by malicious and other actors (Internet Society, 2019[58]). As such, encrypted DNS transport also enhances DNS integrity as it makes it more difficult for third parties to perform DNS spoofing (Wei and Heidemann, 2011[26]).[22] In addition, the deployment of encrypted DNS transport makes it very difficult if not impossible for ISPs and actors other than resolvers to perform DNS blocking and filtering[23].

Despite its clear benefits for DNS confidentiality, the use of encrypted DNS transport also raises significant concerns. While the introduction of encrypted DNS transport can provide point to point confidentiality for DNS queries, its implementation can dramatically change where user query information is handled and who has the ability to act on the data in transit, with potential harmful results for DNS security (SSAC, 2020[40]). In fact, the deployment of encrypted DNS transport has accompanied patterns of emerging concentration in the resolver market, in particular regarding Google's open public resolver (see above). With DNS encrypted transport, the resolver continues to benefit from full access to the data associated with the DNS queries, and there may be limited safeguards regarding the application of national privacy laws (e.g. GDPR) if the resolver processes data in jurisdictions distinct from the user's location, and if no adequacy decisions ensure a similar level of protection.[24] As discussed above, such privacy concerns are reinforced by the fact that there is no financial transaction associated with DNS resolution, and little transparency on how leading open public resolvers process the data associated with DNS queries (Huston, 2021[32]). In other words, a possible way for a for-profit resolver to have a financial interest in providing this "free" service is to exploit the data associated with the user's DNS queries.

In addition, as discussed above, the use of DoH raises significant concerns regarding the increased role of applications in the resolution process. With DoH, applications such as browsers perform DNS queries that are effectively invisible to all other actors, and the choice of the DNS resolver is embedded at the level of the application, as opposed to being made by the ISP or the user (SSAC, 2020[40]). The DNS resolution service at the level of the application can therefore bypass local digital security measures (for instance put in place by network administrators), which may result in significant negative impacts for digital security risk management overall.

To summarize, while the current practices of encrypted DNS transport hold the promise of significant improvements for DNS confidentiality (and for DNS integrity at some level), they also have certain limitations and raise some concerns:

- The current practices of encrypted DNS transport only enhance the confidentiality of the data exchanged through the resolution process between the user and the resolver (as such, they do not enhance security at other levels of the DNS ecosystem);
- While they prevents third parties (e.g. ISPs or malicious actors) to access the encrypted data, the data is still available to the resolver. This may increase digital security risk if the resolver is located in a third country with lower safeguards regarding privacy or security, or where redress mechanisms for privacy protection are not available for the user;
- They also make it difficult for actors such as ISPs or organisations to filter DNS traffic, including to block malicious traffic that can negatively impact users (e.g. malware or the use of DNS as a covert channel, see below). They effectively transfer decision-making for DNS filtering to the resolver.

Other technical solutions to enhance DNS security

In addition to DNSSEC and encrypted DNS transport, other innovative technical solutions are being developed to enhance DNS security, as discussed below.

Query name (QNAME) minimisation (RFC 9156) is an important technical solution that significantly enhances DNS confidentiality for users and resolvers. It is a technique used by resolvers to send the shortest possible name to an authoritative server. In the context of the root zone, this means that resolvers only send the top-level domain (TLD) portion of a particular name. For example, rather than send a fully qualified domain name like 'www.example.com', the resolver can send a query for only 'com'.

Aggressive DNSSEC Caching (RFC 8198) is another confidentiality-enhancing technique that enables a resolver to use DNSSEC data from negative responses to cache the fact that no names exist between a certain range. Future requests can be answered from this cached data, rather than sending another query to an authoritative server. For example, when a resolver learns that the root zone contains no names (TLDs) between '.coop' and '.corsica' then it can avoid sending further queries for non-existent names such as 'mycompany.corp'.

Both QNAME Minimisation and Aggressive DNSSEC Caching provide important confidentiality benefits at all levels of the DNS.

The technical solutions and standards discussed above show that the DNS multi-stakeholder community is active in developing innovative tools to address specific vulnerabilities in the DNS protocol and its implementation. As discussed above, there is no “silver bullet”, and each solution comes with its own trade-offs and potentially negative impact on other economic and social objectives (e.g. technical performance, profitability…) and other aspects of DNS security. However, one may argue that the effective implementation of these technical solutions remains relatively slow, and that current market incentives appear misaligned and may favour the status quo. In addition, the analysis above shows the need to further develop capacity building and education regarding DNS security best practices, in particular for smaller actors of the DNS ecosystem such as some ISPs, authoritative DNS servers at the second and third levels and certain ccTLDs.

Addressing vulnerabilities of DNS actors

To address vulnerabilities of DNS actors that are not “DNS-specific”, there is a need to mainstream digital security risk management best practices for actors of the DNS ecosystem, in particular for those actors that have a role in the registration process (see Figure 5), as suggested by ICANN’s Stability and Security

Review team (SSR2)'s report (SSR2, 2021[22]). This section provides an overview of the key areas where the mainstreaming of best practices could be effective at mitigating vulnerabilities of DNS actors.

Enhancing credentials' security and authentication at the registration level

A promising solution to address the issue of DNS hijacking (see above) is the implementation of a "registry lock", i.e. a set of measures taken by DNS actors of the registration process to add extra authentication steps and to communicate with a registrant before domain settings can be changed. Such steps include multi-factor authentication and the use of services that prevent weak passwords and detect anomalous login patterns (DSFI-TSG, 2021[24]).

In 2019, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an alert calling DNS administrators in the United States to enhance their registrar's authentication settings (CISA, 2019[59]), in particular through:

- Implementing multifactor authentication on domain registrar accounts or other systems used to modify DNS records, where available;
- Verifying that the DNS infrastructure (second-level domains, sub-domains, and related resource records) points to the correct IP addresses or hostnames;
- Searching for encryption certificates related to domains and revoking any fraudulently requested certificates.

Other known best practices to improve the management of credentials include educational programs on digital security risk awareness (e.g. to prevent phishing) and the use of services such as 'Have I Been Pwned' to limit the reuse of compromised password (see Box 3).

Box 3. "Have I been pwned?": the importance of awareness-raising for credentials compromise

The website "have I been pwned?" (https://haveibeenpwned.com) offers an interesting perspective on awareness-raising tools. The name derives from "script kiddie" jargon term "pwn", which means to compromise or take control, specifically of another computer or application.

Created by digital security expert Troy Hunt in 2013, this website could be described as an "*ex post*" (i.e. after a digital security incident) awareness-raising initiative that allows Internet users to check whether their personal data has been compromised by data breaches.

The service collects and analyses hundreds of public databases containing information about leaked accounts, and allows users to search for their own information by entering their username or email address. Users can also sign up to be notified if their email address appears in the future in the databases scanned by the tool.

In 2019, the website had on average 160 000 daily visitors, as well as three million active email subscribers. While not specific to the DNS, this initiative shows how innovative data-mining and communication tools can be developed to raise awareness, sometimes with more effectiveness than traditional approaches.

Source: (OECD, 2021[60])

These are just a few examples of best practices to manage credentials and enhance authentication, which are covered in a wealth of publicly available material (DSFI-TSG, 2021[27]). However, as discussed below, they are not widely implemented by actors of the DNS registration process.

Better addressing code vulnerabilities in the DNS ecosystem.

As outlined above, many attacks targeting DNS actors leverage code vulnerabilities in the software used by these organisations. Often, such attacks involve known vulnerabilities for which a patch or security update is available, but has not been implemented by organisations – as opposed to "zero-day" vulnerabilities (see (OECD, 2021[61]; OECD, 2021[62])).

To address such vulnerabilities, DNS actors must adopt comprehensive digital security risk management strategies, which include for instance regular patching and ceasing to use products that are no longer supported by the software provider (OECD, 2021[60]).

Mainstreaming a strategic approach to digital security risk management.

More broadly, there is a need for actors of the DNS ecosystem to further adopt digital security risk management frameworks. Too often, some stakeholders, in particular some ccTLDs, registrars and resellers, limit their digital security management practice to methodologies such as "checklists" that focus on legal compliance. However, as described below, digital security risk management requires a much more holistic, systematic and cyclical process.

Digital security risk management can be divided into two phases: i) risk assessment and ii) risk treatment (OECD, 2015[63]). More precisely, a risk based approach involves evaluating risk on the basis of its likelihood and severity, based on the context (i.e. risk assessment), and addressing this risk by deciding which part of the risk to accept, mitigate, transfer or avoid (i.e. risk treatment). Risk management frameworks allow organisations to take security measures that are appropriate to and commensurate with the risk, aligned with their internal risk tolerance (also called "risk appetite"), and that do not harm the economic and social activities at stake. As digital security risk is dynamic, risk management must be systematic and cyclical. The NIST Cybersecurity framework provides a good example of a risk-based approach to digital security (see Box 4).

Box 4. The NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a guidance developed in 2014 by the United States' National Institute of Standards and Technology (NIST) that aims to enable organisations to assess and treat digital security risk. It is based on existing international standards, guidelines and practices, and aims to simplify them to make the framework accessible to most organisations. The NIST Cybersecurity framework focuses on five core security activities or functions, that could provide a structure for organisations' digital security risk management strategy:

- Identify, i.e. develop a mapping of the organisation' systems, people, assets, data, and capabilities. This includes understanding the business context, the resources that support critical functions, and the related digital security risks, which enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- Protect, i.e. outline appropriate safeguards to ensure the delivery of the most critical functions.
- Detect, i.e. define the appropriate activities to identify the occurrence of a digital security incident in a timely manner.
- Respond, i.e. take action and contain the impact of a potential digital security incident
- Recover, i.e. develop plans for resilience and to restore the capabilities or services that were impaired due to a digital security incident.

The NIST Cybersecurity Framework provides for each activity a list of industry and international standards that may be used by organisations to assess their maturity.

Source: OECD

2. A more recent trend suggests to complement risk management practices with a "zero trust" approach or model ("zero trust") (DSFI-TSG, 2021[24]; OMB, 2022[64]). Zero trust suggests an evolution in security architecture, which usually relies around a perimeter that needs to be protected. Zero trust implements the principle of "defense-in-depth", while going beyond traditional network boundaries. In fact, zero trust eliminates implicit trust in any one element, node, or service and instead requires continuous verification via real-time data from multiple sources to determine access and other system responses. In essence, a zero trust architecture allows users full access, but only to the bare minimum they need to meet their needs on a case-by-case basis. As a zero trust architecture assumes that a breach is inevitable or has likely already occurred, it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero trust architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment (US government, 2021[65]). Although zero trust, which is based on state-of-the-art risk management, is still emerging, it holds significant potential to increase digital security overall, including for actors of the DNS ecosystem. However, adopting a zero-trust model would make sense for advanced actors that already have put in place effective digital security risk management frameworks.

Significant gaps remain unaddressed

The best practices outlined above are not sufficiently implemented across the DNS ecosystem (DSFI-TSG, 2021[27]). For instance, authentication and credentials management are not harmonised across the DNS ecosystem, and registry lock is not widely deployed yet. Many actors of the DNS ecosystem, in particular certain registrars, ccTLDs and ISPs, lack threat-monitoring capabilities and have not yet deployed a comprehensive risk management framework. In addition, as in other sectors, incidents are often kept secret out of fear of potential ramifications such as legal liability and reputational damages (DSFI-TSG, 2021[27]).

The lack of implementation of digital security risk management best practices across the DNS ecosystem often results from misaligned economic incentives. Limited budgets and other business drivers may lead many organizations in the DNS ecosystem to de-prioritize digital security (DSFI-TSG, 2021[27]). In addition, while registries may have strong security mechanisms, a reseller that acts as an intermediary between registrants and registrars (see above) can be the weakest link as they do not have the same obligations or control requirements as parties that have contractual arrangements with ICANN. More broadly, there is need to enhance digital security risk management and to realign incentives towards that goal at the level of registrars and ccTLDs.

Addressing dependencies and emerging concentration in the DNS ecosystem.

To reduce dependencies and the systemic risk associated with single points of failure, there is a need to support supply chain diversification and to further empower stakeholders to access a variety of suppliers. A more diversified supply chain typically enables a wider range of suppliers to compete, which may then use digital security as a market differentiator. The role of standard development and interoperability is also key, as it can reduce switching costs.

As discussed above, the efforts of the multi-stakeholder community to invest in research and development, undertaken in the 2010s, resulted in the provision of alternative DNS management software, which ended

the monoculture associated with software such as BIND (Huston, 2021[32]).These alternative products are typically developed as open-source software by DNS stakeholders, including for instance “KNOT” developed by the “.cz” registry (CZ.NIC), “Unbound” developed by NLNet and PowerDNS. In that perspective, governments could support the multi-stakeholder community’s efforts and further incentivise DNS stakeholders (e.g. ccTLDs) to invest in specialist skills as well as in research and development.

The emerging concentration in the resolver market is a relatively recent phenomenon.[25] Nevertheless, the multi-stakeholder community has also started to address this specific concern. For instance, Quad9, a non-profit foundation headquartered in Switzerland, was founded in 2016 to provide resolution services coupled with high standards regarding technical performance and digital security (e.g. enabling DNSSEC validation and DoT), as an alternative to for-profit resolution services such as Google’s resolver.

Some governments have also supported, or intend to support, the development by the technical community of open public resolvers headquartered locally, for instance in Canada or in the European Union (see Annex A). The objective of these initiatives is to provide additional safeguards for the application of national law regarding digital security and privacy. However, such initiatives would also have to comply with applicable law regarding DNS-level action to prevent access to content that may be considered as illegal or abusive. This could disincentivise users to switch to these resolvers, as they would not provide more benefits than their ISP’s resolution service. Another avenue for policy action in this area could include a dialogue between governments and local ISPs, whose goal would be to further incentivise ISPs to provide high standards regarding privacy and security for their resolution service (e.g. DNSSEC, DoH, DoT, see above).

6. Insights for policy makers

To conclude, the analysis developed above shows that in addition to the three common misconceptions about the DNS outlined in the beginning of the report, a few more deserve attention:

- **Fourth misconception: easy fixes are available to solve DNS security issues**.

A common application of this misconception is the idea that mandating all DNS operators to implement DNSSEC would secure the DNS ecosystem. However, DNSSEC is only effective on one aspect of digital security (integrity) and is typically applied in only one area of the DNS ecosystem (between resolvers and authoritative servers). In addition, as the DNS is a very complex ecosystem, any tweak in a part of it is likely to have unintended consequences in other parts.

In fact, there are always trade-offs between security and other key economic and social objectives such as technical performance, usability or profitability. Even within the realm of DNS security, technical solutions such as DNSSEC and encrypted DNS transport come with trade-offs.

- **Fifth misconception: nothing can be done to enhance DNS security**.

Quite contrary to this view, and balancing the fourth misconception above, many initiatives have been launched by the multi-stakeholder community involved in the DNS ecosystem to address specific issues related to DNS security, as discussed in this report. At the technical level, this "one-issue-at-a-time" approach has proved successful, and also highlights the complexity of the DNS ecosystem and the difficulty of approaching "DNS security" as a whole. It also underlines that the most effective policy lever for governments would be to support existing multi-stakeholder initiatives to increase DNS security.

- **Sixth misconception: DNS security is only a technical issue calling for technical remedies**.

In fact, economic factors such as misaligned market incentives play a key role in DNS security gaps. While technical solutions are the most effective means to fix vulnerabilities in the DNS protocol itself, their implementation, or lack thereof, are interrelated with economic and social incentives affecting DNS actors. To address vulnerabilities of DNS actors, organisational measures and risk management practices are also fundamental, even though they are not always "technical" *per se* (e.g. digital security training for employees).

The analysis above also highlighted that while there are some emerging best practices, significant digital security gaps remain in the DNS ecosystem. As a result, some governments in OECD countries have launched policies aiming to enhance DNS security (see Annex A).

However, introducing policies or initiatives to address the lack of incentives to enhance DNS security should be done with caution, in order to avoid well-intentioned but ill-designed regulations that may lead to adverse effects. For instance, the French Parliament passed a law in 2016 mandating "IPv6 compatibility" for all "terminal equipment". While there is a widespread consensus amongst stakeholders on the need to accelerate the deployment of IPV6, the law proved to be inapplicable in practice. This led the French government to change the law a few years later and remove this obligation, which was considered disproportionate (OECD, 2021[60]). Similarly, regarding DNS security, mandating the deployment of technical solutions such as DNSSEC or encrypted DNS by law or regulation would likely be ineffective and lead to adverse effects (e.g. insecurity-by-compliance). Certain cases have shown that forced implementation of DNSSEC signing through governmental mandates without sufficient training, capacity building and technical support have led to an increased risk of digital security incidents (e.g. unavailability due to DNSSEC errors, (Rasmussen, 2010[56])).

To avoid these pitfalls, there is a need for governments to:

- Consult the DNS multi-stakeholder community and co-design any initiative regarding DNS security with its members. In particular, governments could work together with their ccTLDs to better

measure and incentivise the adoption of DNS security best-practices such as DNSSEC signing, and with local ISPs to further develop DNSSEC validation and the use of encrypted DNS transport in their DNS resolution services;

- Lead by example with their own DNS infrastructure (e.g. by deploying DNSSEC signing for the authoritative DNS servers managed by the government, at local, regional and national levels);
- Support stakeholder-led initiatives to develop capacity building on DNS security, in particular targeting smaller organisations such as certain ISPs, ccTLDs, registrars and SLDs (e.g. through public funding);
- Promote diversification of the DNS ecosystem and its supply chain, in particular through the development of alternatives for key functions (e.g. DNS management software or resolvers);
- Support research and development in areas where significant technical gaps for DNS security remain unaddressed (e.g. authentication between users and resolvers); and
- Where governmental action is needed, favour technology-neutral, principles-based and outcomes-oriented policies (as opposed to technical requirements). Such policies outline the outcomes that stakeholders should aim to achieve and the main principles that should guide them in achieving these outcomes (e.g. data minimisation for GDPR). While these regulations do not impose specific technical means to achieve these outcomes, they can incentivise or require economic actors to follow recognised international or industry standards[26]. These standards are agile enough to evolve rapidly and cope with the speed of innovation. By setting a general framework, principles-based and outcomes-oriented policies allow stakeholders to choose which international standards or technical specifications are the most appropriate, in their specific context, to enable them to achieve the objectives set in the regulations (OECD, 2021[60]);
- Further co-operate at the international level to enhance the security of the DNS ecosystem, preserve its functioning as a core global infrastructure and avoid Internet fragmentation. In that regard, enabling an international and multi-stakeholder dialogue to better understand and address DNS security challenges is essential.

Annex A. Policies on DNS security

Canada

In April 2020, the Canadian Internet Registration Authority (CIRA), the organisation that manages Canada's ccTLD ".ca", launched its own open public resolver, referred to as "Canadian Shield". The objective of this service is to provide enhanced security and privacy to Internet users in Canada.

Such benefits derive from CIRA's governance structure as a not-for-profit organization – as such, CIRA would have no interest in monetizing the data associated with DNS queries and responses. The Canadian Shield is also the result of a partnership between CIRA and the Canadian Centre for Cyber Security, which intend to share information regarding threat intelligence. CIRA's deployment of a national, public open resolver enabling DNS over HTTPS (DoH) is a first of its kind. (CIRA, 2020[66]).

European Union

The EU Cybersecurity Strategy and the DNS

Launched in December 2020 by the EU Commission, the EU Cybersecurity Strategy outlines new actions related to DNS security, including DNS resolution. The strategy considers that "people and organisations increasingly rely on a few public DNS resolvers" and that "such consolidation of DNS resolution in the hands of few companies renders the resolution process itself vulnerable in case of significant events affecting one major provider, and makes it more difficult to address possible malicious cyberattacks incidents".

To address this risk, the EU Commission plans to further incentivise diversification of DNS resolution and to launch a 'DNS4EU' initiative. The goal of this initiative would be to provide an open public resolver headquartered in the EU, as an alternative to existing open public resolvers. Such resolution service would be compliant with applicable EU law regarding privacy and digital security, and "transparent, conform to the latest security, data protection and privacy by design and by default standards and rules" (European Commission, 2020[3]).

Revision of the EU directive on Network Information Security (NIS)

The EU Network and Information Security (NIS) directive from 2016 provides legal requirements for the digital security of operators of critical activities. Current discussions on the revision of this directive ("NIS2") examine the extent to which its provisions would apply to actors of the DNS ecosystem (European Commission, 2020[67]).

Switzerland

In Switzerland, the ccTLD ".ch" (operated by the registry SWITCH) and the gTLD ".swiss" (operated by the Swiss Government) are subject to a common regulation with regard to the handling of cybercrime cases. This regulation provides, *inter alia*, a clear legal and operational framework for the two registries to co-operate with accredited cybercrime authorities to act swiftly when there is reason to believe that the domain name in question is being used for malware and phishing. In addition, the legal framework in place

mandates the registries to collaborate with the authorities in the event of other abuses (e.g. when a domain name is used for an unlawful purpose or in an unlawful manner).

Annex B. DNS abuse

There is no internationally agreed definition of "DNS abuse". Some stakeholders have adopted an expansive definition of DNS abuse, which would include any illegal website content on the Internet within its scope. Others have adopted a more narrow definition, which describes DNS Abuse as malware, botnets, phishing, pharming, and spam, when it serves as a delivery mechanism for the other four forms of DNS abuse[27] (DNS abuse framework, 2020[21]). A report recently developed within the ICANN multi-stakeholder community considers that DNS abuse can be defined as the "intentional misuse" of domain names "for cybercrime infrastructure" or to direct "users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud" (SSR2, 2021[22]).

In the context of this report, and to distinguish it from DNS security, **DNS abuse** refers to the use of the DNS for malicious purposes, without necessarily resulting in a technical impact on the DNS itself.

DNS abuse may encompass two categories:

- **The use of the DNS in digital security attacks**, impacting the AIC triad of Internet users, without any impact on the DNS itself. Domain names are typically an integral part of phishing campaigns and can be used by malware or for the Command and Control (C2 or C&C) platforms of botnets, i.e. the sets of tools that malicious actors use to communicate with compromised devices. The DNS can also be used as a "covert channel" to allow malicious traffic to flow unnoticed through "DNS tunnelling"; which may also be used for data exfiltration. This category is often referred to as DNS "technical abuse" (I&J, 2021[12]) and may be considered as overlapping in some instances with DNS security.
- **The use of the DNS for other illegal activities**, without any impact at the technical level on the AIC triad of Internet users or parts of the DNS, including the use of domain names to provide access to illegal content (e.g. copyrights infringements, hate speech, violent and extremist content, etc.). This category is often referred to as DNS "content abuse" (I&J, 2021[12]).

As noted above, it should be emphasised that the DNS ecosystem is a neutral, logical layer that exists and operates independently from the underlying websites or services that provide content. What is often labelled as "addressing DNS abuse" should therefore rather be understood as "DNS level action to address abuses online", i.e. leveraging the DNS ecosystem to solve issues that neither affect nor are caused by the DNS specifically (I&J, 2021[12]). In fact, many forms of DNS abuse relate to content and services that belong to the "content layer".

DNS technical abuse

As the DNS is a critical infrastructure underpinning the functioning of the Internet, it is often used by malicious actors in the course of their digital security attacks. However, these attacks typically have no effect on the DNS itself, and are therefore referred to as a form of DNS abuse. Within the multi-stakeholder community, **the use of the DNS in digital security attacks** is often referred to as "DNS technical abuse", and covers the following categories (while not being limited to those) (I&J, 2021[12]; ICANN, 2017[68]):

- **Malware**, i.e. malicious software which is installed on a device and disrupts its operations, for instance by gathering sensitive information (impact on confidentiality), tampering its data (integrity

impact) or making it unusable (availability impact). Malware typically include viruses, spyware and ransomware. Malicious actors can use the DNS to spread malware (e.g. registering a domain name and redirecting it to a website that infects Internet users with malware). They can also use the DNS in the malware's code: for instance, some malware, such as the WannaCry ransomware, have a "kill switch" that relies on the DNS to function (OECD, 2021[31]). Typically, the malware would regularly attempt to connect to a specific domain name: if the domain name is not registered, the malware continues to function, but if the domain name is registered, the malware ceases all activity.

- **Phishing**, i.e. when a malicious actor tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. credentials such as account numbers, login IDs, passwords), typically through sending fraudulent or "look-alike" emails or luring users to copycat websites. Some phishing campaigns also lead users into installing malware. Typo-squatting, i.e. registering domain names that look alike legitimate ones, can be used as a tool to make the phishing campaign more effective (e.g. adding a link to a fictively malicious "oedc.org" in an email impersonating an OECD official). Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information, without any impact on the AIC triad of parts of the DNS (DSFI-TSG, 2021[24]).
- **Botnets**, i.e. collections of devices connected to the Internet that have been infected with malware. Botnets are typically placed under the control of a remote administrator through a Command & Control platform (C2 or CC), which is operated through the DNS (I&J, 2021[12]).
- **DNS as a covert channel**, also known as "DNS Tunnelling", i.e. when DNS query and response channels are used to hide malicious communication, which appears as benign DNS traffic (DSFI-TSG, 2021[24]). Using DNS as communication channel enables exchanges between firewalled resources and external third parties with malicious intent. In fact, since DNS traffic is often allowed to traverse network boundaries largely unimpeded and unmonitored, it is possible to create a two-way communications stream using seemingly innocent DNS queries and responses to pass messages such as requests for instructions or exfiltration of data. For instance, in 2014, malicious actors installed malware on the network of beauty products chain Sally Beauty and managed to exfiltrate financial data (clients' credit cards information) unnoticed by transmitting it as domain name system (DNS) traffic (Krebs, 2014[69]).

DNS content abuse

Beyond DNS security and DNS technical abuse, the DNS may be used for malicious purpose without any impact on the AIC triad of Internet users. In fact, the DNS can be used to map domain names onto IP addresses where illegal or abusive content is hosted. Within the multi-stakeholder community, DNS content abuse is often understood as covering the following categories (while not being limited to those) (I&J, 2021[12]):

- **Child abuse material.**
- **Controlled substances for sale or trade**, including illegal drugs, the illegal sale of legal drugs, illegal services, stolen goods and illegal firearms or other weapons.
- **Violent extremist content,** including content that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups.
- **Hate speech,** including advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.
- **Intellectual property infringements** that relate to website content (not to the domain name itself), including trademarks (e.g. sale of counterfeit goods), patent or trade secret infringement, or piracy of copyrighted works.

The list provided above does not intend to be exhaustive, as what constitutes an "illegal" service or piece of content is likely to significantly differ across jurisdictions. It does not suggest either that the categories listed above are equivalent in terms of malicious impact or would necessitate an equivalent level of response and mitigation by law enforcement or DNS stakeholders.

Addressing DNS abuse: challenges and opportunities

As outlined above, what is often labelled as "addressing DNS abuse" should rather be understood as "DNS level action to address abuses online", i.e. leveraging the DNS ecosystem to solve issues that neither affect nor are caused by the DNS specifically (I&J, 2021[12]). Most forms of DNS abuse relate in fact to content and services that belong to the "content layer" outlined in Figure 1, and should be associated with the content host and the registrant, rather than with actors of the DNS ecosystem. Nevertheless, policies and mechanisms relying on the DNS to address abuses online have been put in place at various levels of both the resolution process and the registration processes. The short argument below outlines that these policies and mechanisms may have unintended consequences that could have an impact on DNS security (i.e. by affecting the availability, integrity or confidentiality of parts of the DNS ecosystem).

Administrative and judiciary measures addressing DNS abuse and impacting the DNS

Because of the cross-border nature of the Internet, it is difficult for governments to act at the level of the content host or of the registrant to address online abuses, as those are often located in different countries with which no legal or technical co-operation framework exists (and if such framework exists, its implementation may be limited or ineffective). As a result, action at the level of the DNS is perceived by some governments as an effective way to reduce online abuses. Such action typically entails requesting DNS actors, in particular ISPs, to block access to content by not resolving certain domain names. Such action is relatively easy to implement for governments because ISPs are typically local companies subject to national law, as opposed to other DNS actors and to actors of the content layer.

However, actors of the DNS ecosystem often consider that it is problematic to treat requests regarding online abuse, in particular content abuse, at the DNS level, as resolvers, registries and registrars (contrary to content hosts) typically cannot technically remove illegal or offending pieces of content from a website or from an online platform. Through DNS blocking, access to the content would be prevented for some users, but the content itself would not be impacted. This is why DNS operators often consider that in these cases, remediation for content abuse should occur at the registrant or content host level (see Figure 1). This reluctance of DNS operators to act at the DNS level is reinforced by the fact that action at DNS level is likely to trigger conflicts of jurisdiction, as the qualification or definition of most of the categories listed above as part of DNS content abuse (e.g. hate speech) is likely to differ across jurisdictions. In other words, the same piece of content or service may be legal in one country and illegal in another.

In addition, addressing abuse at the DNS level tends to result in unintended consequences (SSAC, 2011[1]). For instance, individual users that cannot access certain parts of the DNS may decide to circumvent the blocking by choosing a resolver distinct from their ISP's resolution service, typically an open public resolver such as Google or Cloudfare (Radu and Hausding, 2020[38]). Administrative or judiciary decisions that compel DNS actors (e.g. ISPs or open public resolvers) to block the resolution of or access to certain domain names can cause significant collateral damage, including restricting access to legitimate content (ISOC, 2017[70]; EFF, 2021[71]; Quad9, 2021[72]). For instance, DNS-level measures to take down illegal website content may result in taking down legal content and services that are technically dependent on the targeted domain name. The use of broad DNS abuse blocking measures typically results in making legitimate parts of the DNS ecosystem unavailable, hence having a negative impact on DNS security, and more broadly on human rights such as freedom of expression and access to information. Legal requests

for resolvers to stop resolving certain names for certain categories of users (e.g. located in certain countries) may also have a negative impact on technical performance.

The issue of WHOIS and access to registrants' data

WHOIS is a technical protocol governing the display of certain data relating to the DNS, which usually appear through databases containing information regarding domain name registrants, maintained by actors of the registration process (i.e. registries and registrars). Historically, WHOIS has been extensively used by the security community (e.g. law enforcement, security researchers, etc.) to combat DNS abuse. However, since 2018, the application of the EU General Data Protection Regulation (GDPR) by registries and registrars, and at the level of ICANN and its community, has challenged and modified the design and functioning of the WHOIS database, making it much more difficult for the security community to effectively access certain types of previously public personal information. While before 2018, WHOIS data were more easily accessible by the public, the new WHOIS structure (as of October 2021) relies on registrars and registries to handle requests to access WHOIS data from third-parties (FIRST, 2018[73]; Tech Accord, 2018[74]).

Some stakeholders consider that the new design and functioning of WHOIS result from a "misapplication" of GDPR (Tech Accord, 2021[75]), and do not sufficiently balance registrants' privacy with other important policy objectives such as security. For instance, contact details for registrants such as email addresses are no longer easily accessible through the WHOIS. Similarly, the current proposed design of WHOIS for gTLDs does not require registrars and registries to make a distinction between physical (or "natural") persons (whose privacy is protected by GDPR) and legal persons (that are not subject to GDPR), whereas such distinction is made in the WHOIS of some European ccTLDs. As a result, some stakeholders consider that up to 98% of WHOIS access requests are either denied or unanswered, resulting in an increasing reliance on other mechanisms to address abuse, for instance requests of DNS filtering at the level of ISPs and resolvers (Felman, 2021[76]; Tech Accord, 2021[75]). On the other hand, other stakeholders consider that the *status quo* that existed prior to the GDPR put registrants at risk of becoming victims of identity theft, spamming, spoofing, online harassment, and even offline targeted harm.

The example of WHOIS shows how visibility and accountability, which are key components of effective digital security risk management, may negatively affect confidentiality and privacy. However, this topic is not directly in the scope of this report.

Multi-stakeholder initiatives to address DNS abuse

Setting aside the impact of legal and governmental measures, it is worth noting that actors of the DNS ecosystem have put in place mechanisms and policies to reduce DNS abuse, in particular by using two methods:

- Preventative approaches, which involve the detection of potentially harmful domains as part of the process of registration, and result in either preventing the registration from completing, or preventing the domain from resolving for some time. Potentially harmful domains can be identified via:
  - Attributes of the domain name itself (e.g. domains that present a significant likelihood of intentional typo-squatting);
  - Attributes of the registrant (links to other harmful domains, payment intelligence, email);
  - Attributes of the transaction (number of domains, payment method).
- Reactive methods, which involve the identification of a harmful domain after both registration and malicious activity have occurred. This identification is typically done via two tools:

- Direct abuse reports to the registrar or registry, including for instance through Trusted Notifiers programs;
- Through a Reputation Block List (RBL) or abuse feed to which the registrar or registry subscribes. RBLs and abuse feed providers usually build their data sets through a combination of monitoring, searching, and direct reports of abuse.

However, as noted in a recent report (SSR2, 2021[22]), there is a lack of harmonisation regarding the application of these methods across both registries and registrars. The time taken to review and process an abuse report and the extent of resources allocated to reducing abuse significantly differ across actors of the registration process.

In addition, available data (see below) suggests that a limited number of registries and registrars play a significant role in allowing DNS abuse at scale, without taking sufficient measures to address abuse cases. While this data is available, there is little evidence regarding effective actions taken to realign incentives for registries and registrars that do not put in place sufficient mechanisms to address abuse. For gTLDs, such action could take place at the level of the ICANN community (e.g. name and shame mechanisms, financial sanctions…) while for ccTLDs, action could be taken by the government responsible for the country or territory.

From another perspective, it could be argued that an expeditious treatment of abuse reports could lead to DNS security issues, e.g. a breach of availability from the registrant's point of view. As a result, it is important that stakeholders (e.g. in governments and in the DNS registration and resolution processes) give sufficient due process to any abuse report (I&J, 2021[12]).

To tackle these challenges, several important initiatives have been launched over the last few years to gather data on DNS abuse and foster collaboration to reduce it. Such initiatives include:

- The Internet & Jurisdiction policy network's domain track, which provides a recognised platform that allows stakeholders to discuss and make progress on a common understanding of what DNS abuse is and on the best practices to address it (I&J, 2021[12]).
- ICANN's DAAR and ITHI projects, which provide data on DNS abuse (see Box 1),
- The "Spamhaus" initiative (https://www.spamhaus.org), which provides RBLs and features a list of the top ten "most abused" TLDs, defined as registries that allow registrars to knowingly sell high volumes of domains to "professional spammers" and "malware operators". As of October 2021, the top 5 most abused TLDs according to Spamhaus comprised two "new" gTLDs, ".work" and ".surf", and three ccTLDs, ".cn", ".tw" and ".gq" (Spamhaus, 2021[77]).
- The DNS abuse Institute, launched in 2020 to facilitate co-operation, education and innovation in the area of reducing DNS technical abuse (see Box 5).

Box 5. The DNS abuse institute

The Domain Name System (DNS) Abuse Institute (DNSAI) was launched in February 2021 with a mission to reduce the use of the DNS for digital security attacks, e.g. through botnets, pharming, phishing, and the distribution of malware, collectively known as DNS technical abuse. The DNSAI was created and is supported by Public Interest Registry (PIR), the registry operator for the .org TLD.

The creation of DNSAI highlights the DNS ecosystem's growing awareness of the need to do more to address DNS technical abuse. In particular, DNSAI intends to provide analysis and to facilitate the harmonisation of anti-abuse practices across the DNS ecosystem, including registrars and registries of gTLDs and ccTLDs. The DNSAI also intends to address the barriers that limit the effectiveness of anti-

abuse policies and initiatives, such as the difficulty of implementing solutions that require the alteration of domain registration platforms and the lack of economic and social incentives to adopt best practices.

The DNSAI roadmap focuses on three pillars, education, collaboration, and innovation:

- Education: DNSAI develops and distributes guides, primers, best practices, and webinars on DNS Abuse. These resources are targeted towards registries and registrars, law enforcement, businesses large and small, intellectual property and Internet security professionals, and users.
- Collaboration: DNSAI engages with the communities it wishes to serve and provides them with opportunities to give input on the work. It will also be providing a mechanism for the DNS industry to share intelligence and best practices for mitigating abuse.
- Innovation: DNSAI is developing tools for improving preventative and reactive approaches to mitigating DNS abuse, including a Centralized Abuse Reporting Tool (CART). DNSAI also intends to provide data, research, and evidence-based analysis of DNS Abuse.

Source: https://dnsabuseinstitute.org/

This section has helped clarify the distinction between DNS security on one hand and DNS abuse on the other hand. It also points to the relationship between DNS security and measures intended to address abuse, showing that disproportionate anti-abuse measures (e.g. broad DNS-level blocking measures) could have unintended consequences (e.g. incentivising users to switch to open public resolvers) and also negatively affect DNS security (e.g. by making legitimate parts of the DNS ecosystem unavailable, including legal content or services). While addressing online abuses is a legitimate and important public policy goal, it should therefore be pursued with caution and includes impact assessments, in particular when action is taken at the DNS level, as recently outlined by the Internet & Jurisdiction Network (I&J, 2021[12]).

References

Afilias (2009), *Bind 9 vulnerability*, https://circleid.com/posts/afilias_secures_millions_of_internet_domains_from_bind_9_vulnerability/. [36]

Afnic (2021), *Charte de nommage*, https://www.afnic.fr/wp-media/uploads/2021/07/afnic-charte-de-nommage-2021-09-15.pdf. [13]

APNIC (2021), *DNSSEC Validation rate*, https://stats.labs.apnic.net/dnssec. [52]

Bates et al. (2018), *EVIDENCE OF DECREASING INTERNET ENTROPY: THE LACK OF REDUNDANCY IN DNS RESOLUTION BY MAJOR WEBSITES AND SERVICES*, https://www.nber.org/system/files/working_papers/w24317/revisions/w24317.rev0.pdf. [80]

Cimpanu (2020), *Russia TLS*, https://www.zdnet.com/article/russia-wants-to-ban-the-use-of-secure-protocols-such-as-tls-1-3-doh-dot-esni/. [88]

CIRA (2020), *Canadian Shield*, https://www.cira.ca/cybersecurity-services/canadian-shield. [66]

CISA (2019), *DNS Infrastructure Hijacking Campaign*, https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign. [59]

Cisco (2018), “DNSpionage campaign targets Middle-East”, https://blogs.cisco.com/security/talos/dnspionage-campaign-targets-middle-east. [6]

Cloudfare (2021), *Facebook Outage*, https://blog.cloudflare.com/october-2021-facebook-outage/. [82]

Cloudfare (2020), *What is DNS*, https://www.cloudflare.com/learning/dns/what-is-dns/. [78]

Cloudfare (2016), “What is anycast?”, https://www.cloudflare.com/learning/cdn/glossary/anycast-network/. [81]

Cornell (2002), *Root attack*, https://www.cs.cornell.edu/people/egs/beehive/rootattack.html. [47]

DNS abuse framework (2020), *DNS abuse framework*, https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf. [21]

DSFI-TSG (2021), , https://www.icann.org/en/system/files/files/presentation-day1d-dsfi-panel-kaeo-25may21-en.pdf. [27]

DSFI-TSG (2021), *DSFI-TSG report*, https://community.icann.org/display/DSFI/DSFI+TSG+Final+Report?preview=/176623416/176623417/DSFI-TSG-Final-Report.pdf. [24]

EFF (2021), *DNS provider hit*, https://www.eff.org/fr/deeplinks/2021/07/dns-provider-hit-outrageous-blocking-order-your-provider-next. [71]

European Commission (2020), *Proposal for directive on measures for high common level of cybersecurity across the Union*, https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union. [67]

European Commission (2020), *The EU's Cybersecurity strategy for the Digital Decade*, https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade. [3]

Facebook (2021), *Outage details*, https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/. [9]

Felman (2021), *WHOIS*, https://circleid.com/posts/20210223-cybersecurity-accord-98-of-registrar-whois-requests-unrequited/. [76]

FIRST (2018), *GDPR and WHOIS*, https://www.first.org/blog/20180412_GDPR_and_WHOIS. [73]

GAC (2005), *Principles and guidelines for the delegation and administration of ccTLDs*, https://gac.icann.org/principles-and-guidelines/public/principles-cctlds.pdf. [15]

GCSC (2018), *DEFINITION OF THE PUBLIC CORE*, https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf. [2]

Hopkins and Byers (2020), *GhostDNS*, https://team-cymru.com/blog/2020/09/08/illunimating-ghostdns-infrastructure-part-1/. [28]

Huston (2022), *dns4eu*, https://blog.apnic.net/2022/02/11/opinion-dns4eu/. [35]

Huston (2021), "IDS Presentation", https://www.icann.org/en/system/files/files/presentation-day1b-resolver-centrality-huston-25may21-en.pdf. [32]

Huston (2019), "DNS Resolver Centrality", https://blog.apnic.net/2019/09/23/dns-resolver-centrality/. [37]

I&J (2021), *Toolkit: DNS level action to address abuses*, https://www.internetjurisdiction.net/news/toolkits. [12]

IANA (2021), "Root file", https://www.iana.org/domains/root/db. [14]

Ians (2020), *China SNI*, https://www.expresscomputer.in/internet/china-starts-blocking-https-connections-with-encrypted-sni-report/62145/. [87]

ICANN (2021), *Country Focus Report: Russia*, https://www.icann.org/en/system/files/files/ge-006-19jan21-en.pdf. [4]

ICANN (2021), *DAAR*, https://www.icann.org/octo-ssr/daar. [18]

ICANN (2021), *DSFI-TSG*, https://community.icann.org/display/DSFI. [84]

ICANN (2021), *ITHI*, https://www.icann.org/en/system/files/files/octo-025-08jul21-en.pdf. [83]

ICANN (2021), *ITHI dashboard*, https://ithi.research.icann.org/. [39]

ICANN (2020), *DNSSEC deployement in gTLDs*, https://www.icann.org/news/announcement-2020-12-23-en. [50]

ICANN (2020), *ITHI DNS ABUSE*, https://ithi.research.icann.org/graph-m2.html. [17]

ICANN (2019), *What is DNSSEC*, https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en. [5]

ICANN (2017), "Base gTLD Registry Agreement", https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html#specification11. [68]

ICANN (n.d.), *ccTLD agreements*, https://www.icann.org/resources/pages/cctlds/cctlds-en. [16]

IETF (2021), *RFC 9076*, https://datatracker.ietf.org/doc/html/rfc9076. [11]

IETF (2018), *RFC 8484*, https://datatracker.ietf.org/doc/html/rfc8484. [57]

IETF (2013), *RFC 6973. Privacy Considerations for Internet Protocols*, https://tools.ietf.org/html/rfc6973. [25]

IETF (2004), *RFC3833*, https://datatracker.ietf.org/doc/rfc3833/. [23]

Imperva (n.d.), "DNS flood attacks", https://www.imperva.com/learn/ddos/dns-flood/. [20]

Internet Society (2019), *Introduction to DNS Privacy*, https://www.internetsociety.org/resources/deploy360/dns-privacy/intro/. [58]

Internet Society (2014), *The two sides of DNSSEC*, https://www.internetsociety.org/resources/deploy360/2014/the-two-sides-of-dnssec-signing-and-validation/. [49]

ISOC (2019), *Consolidation in the Internet economy*, https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/. [34]

ISOC (2017), *Internet Content Blocking*, https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/. [70]

Krebs (2015), *Hijack of Lenovo domain*, https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/. [33]

Krebs (2014), *Sally Beauty Breach*, https://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/. [69]

Madoury, D. (2021), *Facebook 2021*, https://www.kentik.com/blog/facebooks-historic-outage-explained/. [8]

Mercer and Rascagneres (2019), *DNS on fire*, https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Mercer-Rascagneres.pdf. [10]

Mimoso (2013), , https://threatpost.com/service-restored-to-cn-domain-after-large-ddos-attack/102088/. [29]

Moura, D. et al. (2016), *Anycast vs DDoS*, https://doi.org/10.1145/2987443.2987446. [48]

Netnod (2020), *What are root nameservers?*, https://www.netnod.se/i-root/what-are-root-name-servers. [43]

OECD (2021), *Encouraging vulnerability treatment: background report - Responsible management, handling and disclosure of vulnerabilities*, https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf. [62]

OECD (2021), *Encouraging vulnerability treatment: overview for policy makers*, https://www.oecd.org/sti/ieconomy/security.htm. [61]

OECD (2021), "Enhancing the digital security of products: A policy discussion", *OECD Digital Economy Papers*, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en. [60]

OECD (2021), "Understanding the digital security of products: An in-depth analysis", *OECD Digital Economy Papers*, No. 305, OECD Publishing, Paris, https://doi.org/10.1787/abea0b69-en. [31]

OECD (2018), *Going Digital in Sweden*, https://doi.org/10.1787/9789264302259-en. [55]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://doi.org/10.1787/9789264245471-en. [63]

OECD (Forthcoming), *Security of Routing*. [19]

OMB (2022), *Federal Zero Trust Strategy*, https://zerotrust.cyber.gov/federal-zero-trust-strategy/. [64]

Packet Clearing House (2021), *Root servers global distribution*, https://www.pch.net/ixp/summary_root_servers. [45]

Palo Alto Networks (2020), *Securing Mobile Network Infrastructures: The Need for Constant Real-Time Visibility and Enforcement*, https://www.paloaltonetworks.com/resources/whitepapers/securing-mobile-network-infrastructures.html. [89]

PowerDNS (2019), *Centralised DoH is bad for privacy*, https://blog.powerdns.com/2019/09/25/centralised-doh-is-bad-for-privacy-in-2019-and-beyond/. [79]

Quad9 (2021), *Quad9 files objection opposing sony music german court ruling*, https://www.quad9.net/fr/news/blog/quad9-files-official-objection-opposing-sony-music-s-german-court-ruling/. [72]

Quad9 (2021), *Sony*, https://www.quad9.net/fr/news/blog/quad9-files-official-objection-opposing-sony-music-s-german-court-ruling/. [86]

Radu and Hausding (2020), "Consolidation in the DNS resolver market – how much, how fast, how dangerous?", https://doi.org/10.1080/23738871.2020.1722191. [38]

Rasmussen (2010), *DNSSEC implementation challenges*, https://www.securityweek.com/implementation-challenges-dnssec. [56]

RIPE NCC (2020), *Response to the EU's Cybersecurity Strategy for the Digital Decade*, https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-the-eu2019s-cybersecurity-strategy-for-the-digital-decade. [46]

Root-servers.org (n.d.), *Root server instances*, https://root-servers.org/. [44]

SIDN (2020), *DNSSEC*, https://www.sidn.nl/en/news-and-blogs/dnssec-adoption-heavily-dependent-on-incentives-and-active-promotion. [53]

Sozeri (2015), *Turkey DDOS attack*, https://www.dailydot.com/debug/turkey-ddos-attack-tk-universities/. [30]

Spamhaus (2021), *Spamhaus*, https://www.spamhaus.org. [77]

Spring and Metcalf (2014), *Cache poisoning*, https://insights.sei.cmu.edu/blog/probable-cache-poisoning-of-mail-handling-domains/. [85]

SSAC (2020), "SSAC Report on the Implications of DNS over HTTPS and DNS over TLS", https://www.icann.org/en/system/files/files/sac-109-en.pdf. [40]

SSAC (2011), *DNS blocking: benefits v. harm*, https://www.icann.org/en/system/files/files/sac-050-en.pdf. [1]

SSR2 (2021), *Report*, https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf. [22]

Statcounter (2021), *Operating systems for mobile*, https://gs.statcounter.com/os-market-share/mobile/worldwide. [42]

StatDNS (2022), *StatDNS*, https://www.statdns.com/. [51]

Statista (2021), *Browser market*, https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/. [41]

Tech Accord (2021), *WHOIS counting*, https://cybertechaccord.org/whois-counting-the-cybersecurity-tech-accord-response-to-icanns-most-recent-recommendations/. [75]

Tech Accord (2018), *WHOIS access*, https://cybertechaccord.org/mechanism_to_access_whois_data/. [74]

Traficom (2020), *DNSSEC in Finland*, https://www.traficom.fi/en/news/traficom-promotes-deployment-dnssec. [54]

US government (2021), *Executive Order on Improving the Nation's Cybersecurity*, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. [65]

Wei and Heidemann (2011), *Whac-A-Mole: Six Years of DNS Spoofing*, https://arxiv.org/pdf/2011.12978.pdf. [26]

Wired (2019), "Sea Turtle DNS hijacking", https://www.wired.com/story/sea-turtle-dns-hijacking/. [7]

End Notes

[1] Issues related to security of routing, including BGP, are discussed in [DSTI/CDEP/CISP/SDE(2021)4].

[2] One approach to describe the Internet' structure is to distinguish the physical layer (e.g. fibre), the logical layer (e.g. protocols such as the DNS) and the content layer (e.g. a website).

[3] E.g. by stopping to use the DNS or by building an alternative DNS at the national level (see (ICANN, 2021[4])).

[4] Typically, State-sponsored attacks are motivated by geopolitical interests, while cybercriminals are primarily seeking financial gains.

[5] Even though the term "buy" is commonly used for domain names, the term "lease" is more accurate as the transaction typically results in the registrant obtaining a right-of-use of a domain name for a specific and limited period.

[6] Other categories could also be discussed, such as sponsored TLDs or brand TLDs. However, this is not in the scope of this report, as those categories do not pertain directly to DNS security. In addition, at the technical level, ccTLDs and gTLDs are similar. The key difference between the two is that they are subject to different policies, as ICANN develops policies that apply to gTLDs (through the GNSO) to which ccTLDs are not subject to. Usually, ccTLDs are subject to legal frameworks in place in the country or territory they are associated with (when such framework exists).

[7] There may be however exceptions, in the case where the ccTLD policy issue or the mechanisms set to address it would have an international impact. Then, international frameworks to address ccTLD policy issues may be developed.

[8] DNS hosts belong to the logical layer of the DNS, while "content" hosts such as web-hosting servers rather belong to the content layer. Registrars and resellers may also be content host providers.

[9] ICANN Bylaws state that the organisation "shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide", Art. 1.1(c).

[10] For example, in NXDOMAIN flood attacks, malicious actors flood the DNS server with requests for records that are invalid. The DNS server then uses all its resources to find these records and eventually has no resources left to serve legitimate requests (Imperva, n.d.[20]).

[11] According to the DNS abuse framework, with this definition, generic unsolicited e-mail alone would not constitute DNS abuse. It would only constitute DNS Abuse if that e-mail is part of a phishing scheme.

[12] However, many experts consider that had the DNS been designed in 2021, it would have most likely resulted in the same vulnerabilities. In other words, rather than being a legacy, DNS-specific vulnerabilities result from technical constraints inherent to the functioning of the Internet.

[13] OpenDNS started to provide such services in 2006.

[14] It should be highlighted that contrary to Google and Cloudfare, two for-profit companies headquartered in the United States, Quad9 is operated by a not-for-profit foundation headquartered in Switzerland.

[15] However, should this 70% aggregated market share be distributed across ISPs, each ISP would account for a relatively small market share (below 1% for most ISPs, up to 4-5% for the largest ISPs).

[16] These market players are followed by a long tail of many other open resolvers (up to 6 million), the vast majority of which being inadvertently open due to misconfigurations (Huston, 2021[32])).

[17] However, there have been recent cases of legal proceedings against open resolvers, in which copyrights holders sue open resolvers so that they stop resolving certain names associated with DNS content abuse. See, for instance, the Sony court case against Quad9 in Germany (Quad9, 2021[86]).

[18] Contrary to encrypted DNS transport such as DoT and DoH, DNSSEC does not encrypt DNS traffic (or more precisely DNS queries and responses). It merely enables the use of digital signatures based on cryptographic keys.

[19] In particular, when discussing « rates » of DNSSEC-signed sub-level domains, there is no consensus on which denominator would be the most relevant : one could retain all second-level domains for a specific TLD (but this information is often unavailable), or the most visited second-level domains. The issue of « parked domains » (i.e. domain names that are registered but not used or associated with a website or service) also challenges the measurement of DNSSEC signing. In addition, in some cases measurement of third-level domains makes more sense (e.g. for TLDs using second-level TLDs for specific categories).

[20] See above.

[21] DoT and DoH only provide encryption for the transport channel for DNS queries and responses, but do not make any changes to the DNS protocol itself.

[22] In addition, the authentication function in TLS allows a client to verify the identity of the server. As a result, redirection routing attacks would fail due to the inability of the masquerading resolver to pass the TLS identity verification check.

[23] This had led some governments such as the People's Republic of China (Ians, 2020[87]) and the Russian Federation (Cimpanu, 2020[88]) to consider adopting measures to ban the use of encrypted DNS transport.

[24] E.g. in the case of Cloudfare or Google, from the perspective of a European user switching from their ISP's resolver to Cloudfare or Google's resolver.

[25] In addition, this increased concentration is only emerging within specific segments of the DNS, and as outlined in What is the DNS?, the DNS ecosystem overall is still largely distributed.

[26] For instance, Article 32 of the GDPR ("Security of processing"), states that data processors should take into account the "state of the art" to "implement appropriate technical and organisational measures to ensure a level of security".

[27] According to the DNS abuse framework, with this definition, generic unsolicited e-mail alone would not constitute DNS abuse. It would only constitute DNS Abuse if that e-mail is part of a phishing scheme.