

E-Paper

All about domains 2024



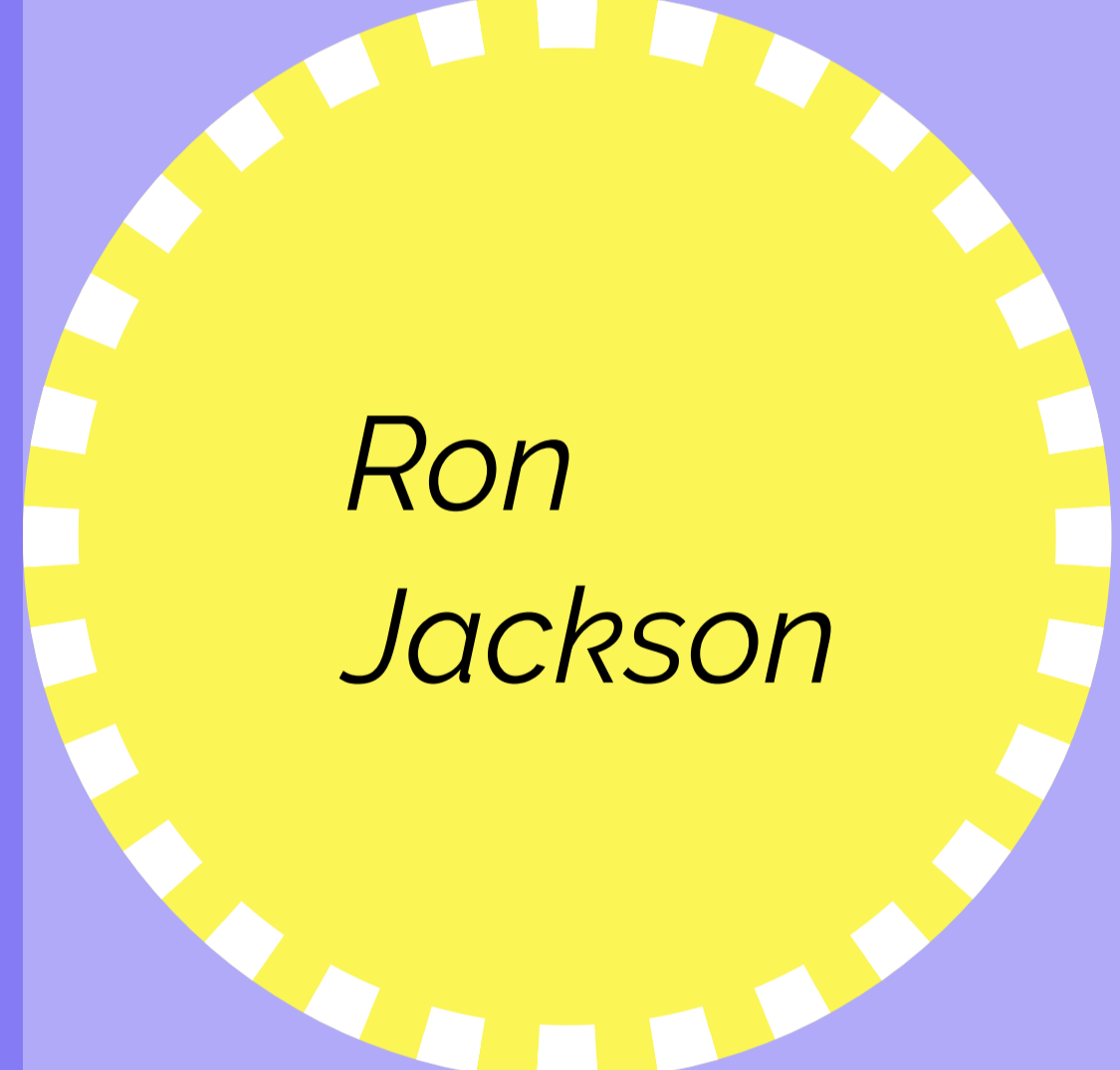
Joe Alagna



Sophie Pieck



Neha Raik



Ron Jackson



Elias Rendón Bengier



Giovane Moura



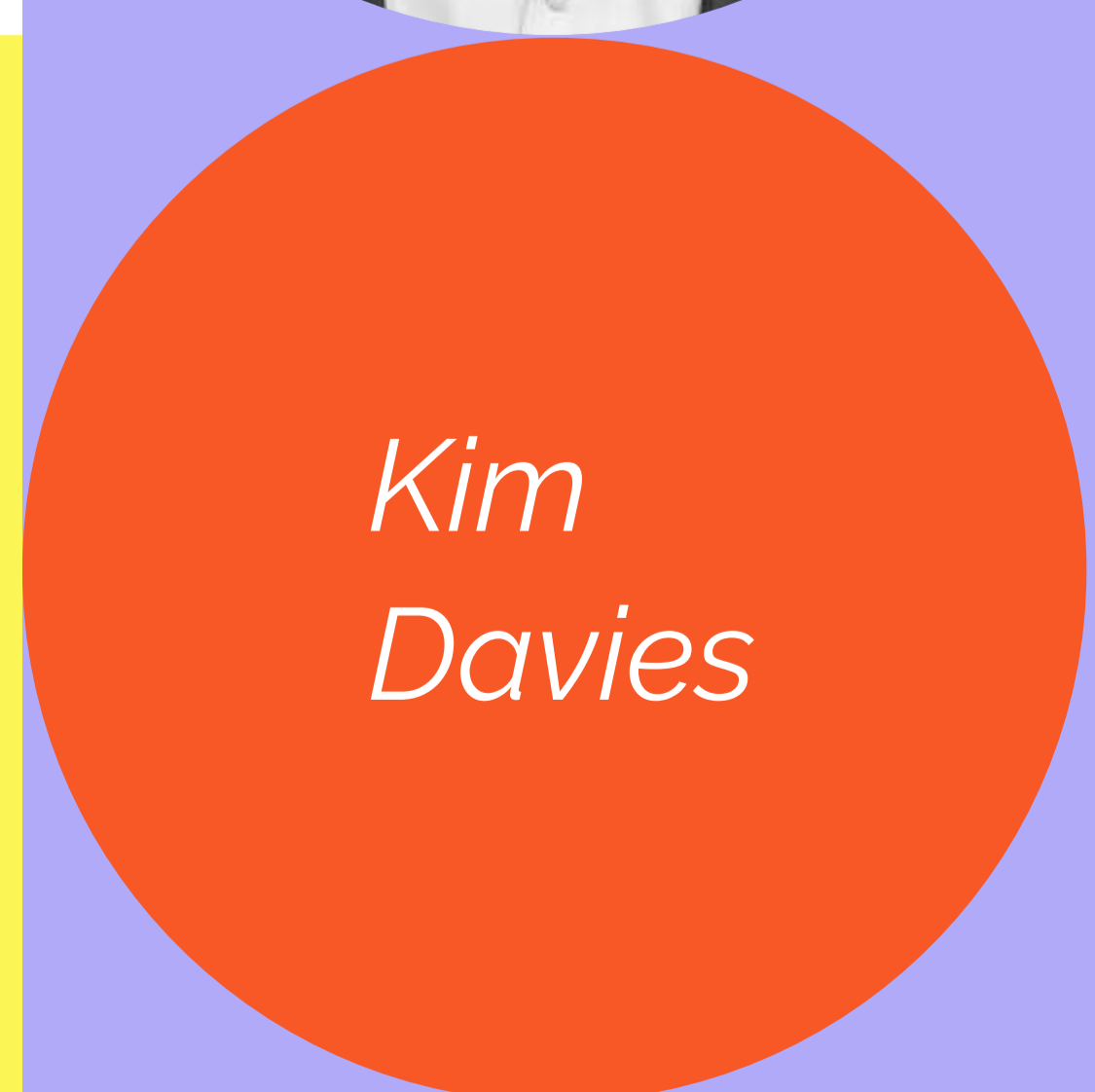
Kelly Hardy



Robert Šefr



Polina Malaja



Kim Davies

It's all about domains ...

► *The domain industry encompasses a diverse and ever-expanding array of niches and domain names are valuable digital assets that open doors to a multitude of possibilities. They serve as critical tools for branding, a smart investment or a security factor in the competitive online space.*

As this sector continues to grow rapidly, it requires the keen insight and strategic foresight of industry experts to successfully navigate its complex dynamics and capitalize on the potential it holds.

In 2021, we launched a project titled "It's all about domains" — an interview series with the vision of convening the leading voices in the domain industry to shed light on its niche and multifaceted corners. Why did we embark on this venture? To forge connections, to foster knowledge sharing and to bridge audiences from disparate industry niches. Our aim was to create a platform where experts could share their expertise, while presenting their personal stories, their achievements and their challenges in shaping the domain landscape we navigate today.

Here we are in 2024 with the third volume, poised to present ten interviews that delve into diverse topics ranging from internet infrastructure and policy to domain investing and DNS security. We are thankful to each expert who has devoted their time and shared their insights. Their contributions have been nothing short of foundational in building the edifice of knowledge this series represents.



Authored by

Simone Catania
Global Content &
Communications Manager

InterNetX

► Immerse yourself in the interviews that define "It's all about domains Vol.3".

Table of contents

01

Kim Davies
IANA*"IANA functions"*

06

Polina Malaja
CENTR*"Internet policy"*

02

Robert Šefr
Whalebone*"DNS4EU"*

07

Kelly Hardy
iQ*"Domain industry"*

03

Joe Alagna
it.com*"it.com domains"*

08

Ron Jackson
DN Journal*"Domain investment"*

04

Sophie Pieck
Sedo*"Domain aftermarket"*

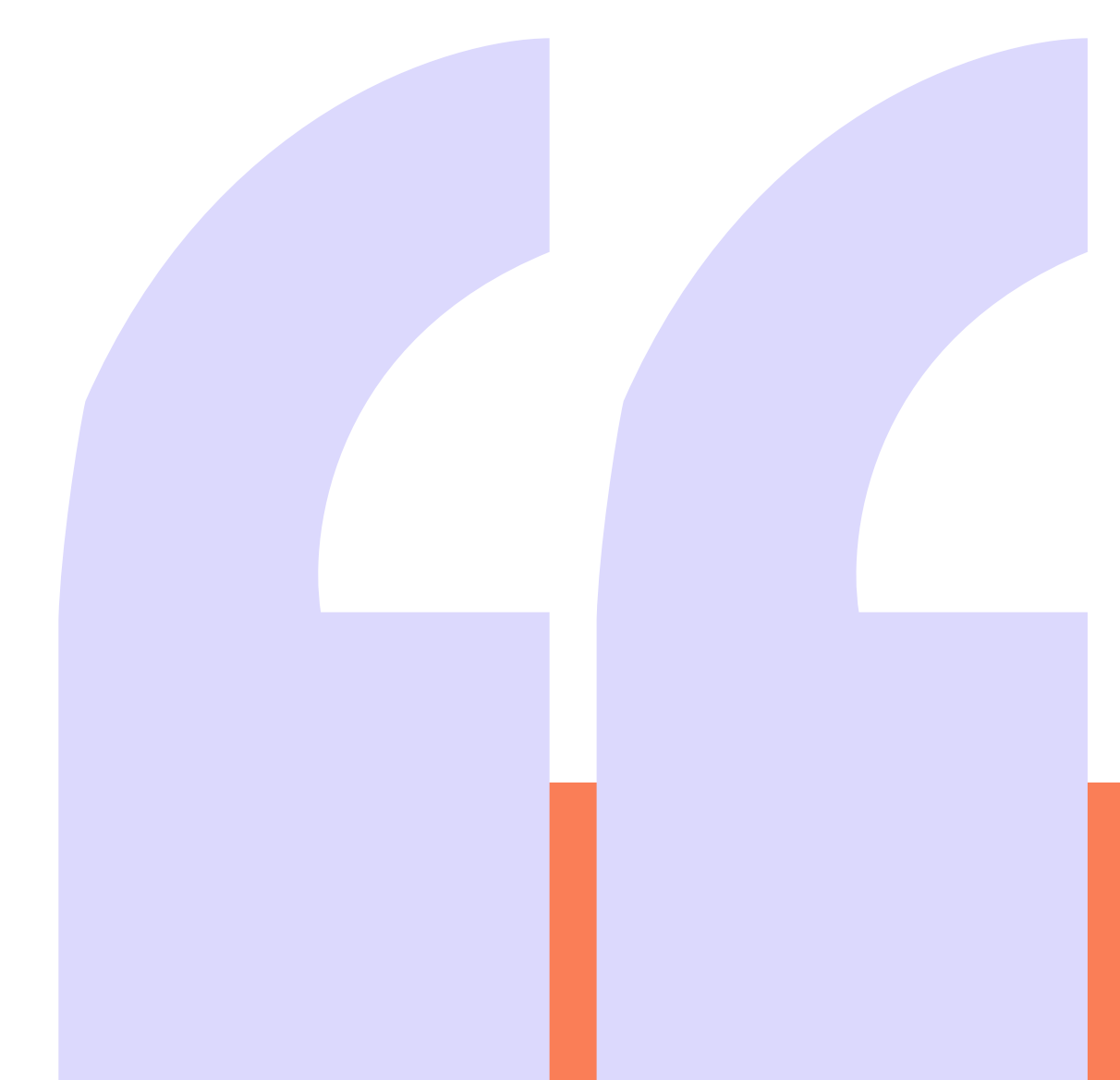
09

Neha Raik
Radix*"Registry business"*

05

Giovane Moura
SIDN Lab*"DNS research"*

10

Elias Rendón Benger
InterNetX*"Domain industry"*



Kim Davies

IANA, VP IANA Services & President PTI

Internet interoperability is at the heart of our connected world. It enables devices, services and systems to communicate and cooperate seamlessly, regardless of the technologies they use or the networks they are connected to. This essential interoperability is made possible through the coordination of unique identifiers, which ensure that everything on the internet has a distinct and recognizable identity. IANA, short for the Internet Assigned Numbers Authority, is the coordination entity in charge of this pivotal role. It manages and coordinates internet identifiers to ensure the internet's stability, security and smooth functioning. IANA's responsibilities are vast and essential for the internet's daily operations, from domain names and IP addresses to protocol parameters and global resource allocation.

Kim Davies, a seasoned internet identifier and governance professional, spearheads operations at IANA as Vice President of IANA Services and President of Public Technical Identifiers (PTI).

With a tenure at ICANN that dates back to 2005, Kim has been instrumental in driving the evolution of IANA. He has pioneered the implementation of technical systems, formalized business processes and introduced quality management practices. Additionally, his efforts have successfully transitioned IANA functions from a US Government contract to a multistakeholder oversight model, further enhancing the inclusivity and transparency of this vital internet governance entity.

IANA PLAYS A CRITICAL ROLE FOR THE DNS



Our primary responsibility is maintaining the authoritative registry for the root zone, the uppermost part of the DNS.

Throughout this interview, we will gain Kim's insights into the challenges and opportunities in managing unique identifiers and fostering internet interoperability and his vision for the future of the internet. So, grab a seat and join us as we embark on this enlightening conversation with Kim Davies, Vice President of IANA Services and President of PTI.

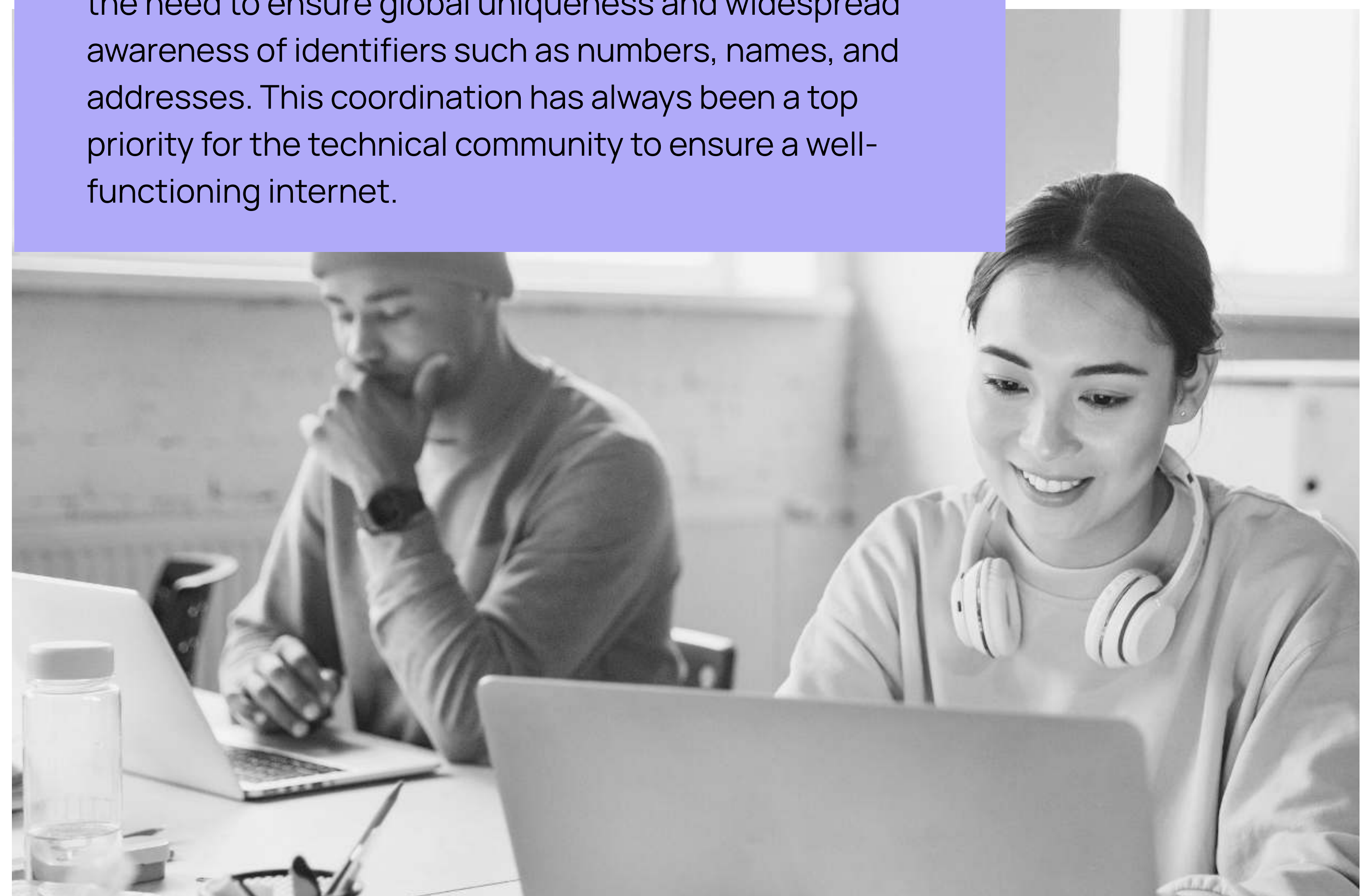
1 *When was IANA established and what key events and milestones have shaped its development over the years?*

The Internet Assigned Numbers Authority (IANA) has a rich history that dates back to the 1970s. A single researcher, Jon Postel, initially managed names, numbers and protocol parameters necessary for internet interoperability, becoming the central authority for assigning and keeping track of identifiers.

With the shift to TCP/IP in 1983 and the growth of the network, the IANA functions gained renewed importance. As the internet grew and evolved, with new assignments and protocols emerging, it became evident that a single person couldn't handle all this work alone and a more structured oversight system was required.

In 1988, the term "Internet" gained popularity during the shift from ARPANET to Internet. This transition involved connecting various networks from different regions to form a unified TCP/IP backbone and the term "Internet" became widely used to describe this interconnected "network of networks." IANA's role in overseeing and managing the Domain Name System (DNS) was officially acknowledged in RFC 1591. According to this Comment, IANA was responsible for coordinating and managing the DNS.

Since its early days, the internet community recognized the need to ensure global uniqueness and widespread awareness of identifiers such as numbers, names, and addresses. This coordination has always been a top priority for the technical community to ensure a well-functioning internet.



The Internet Assigned Numbers Authority (IANA) is responsible for the overall coordination and management of the Domain Name System (DNS), and especially the delegation of portions of the name space called top-level domains.

[RFC 1591, March 1994](#)

By the mid-1990s, the community recognized the need for a more formal, multistakeholder oversight system. Consequently, in 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was established as the designated body, becoming the home of IANA functions in 1999.

2 What is the role of IANA within the DNS ecosystem?

IANA has always played a fundamental role within the DNS ecosystem. Our primary responsibility is maintaining the authoritative registry for the root zone, which is considered the uppermost part of the DNS hierarchy.

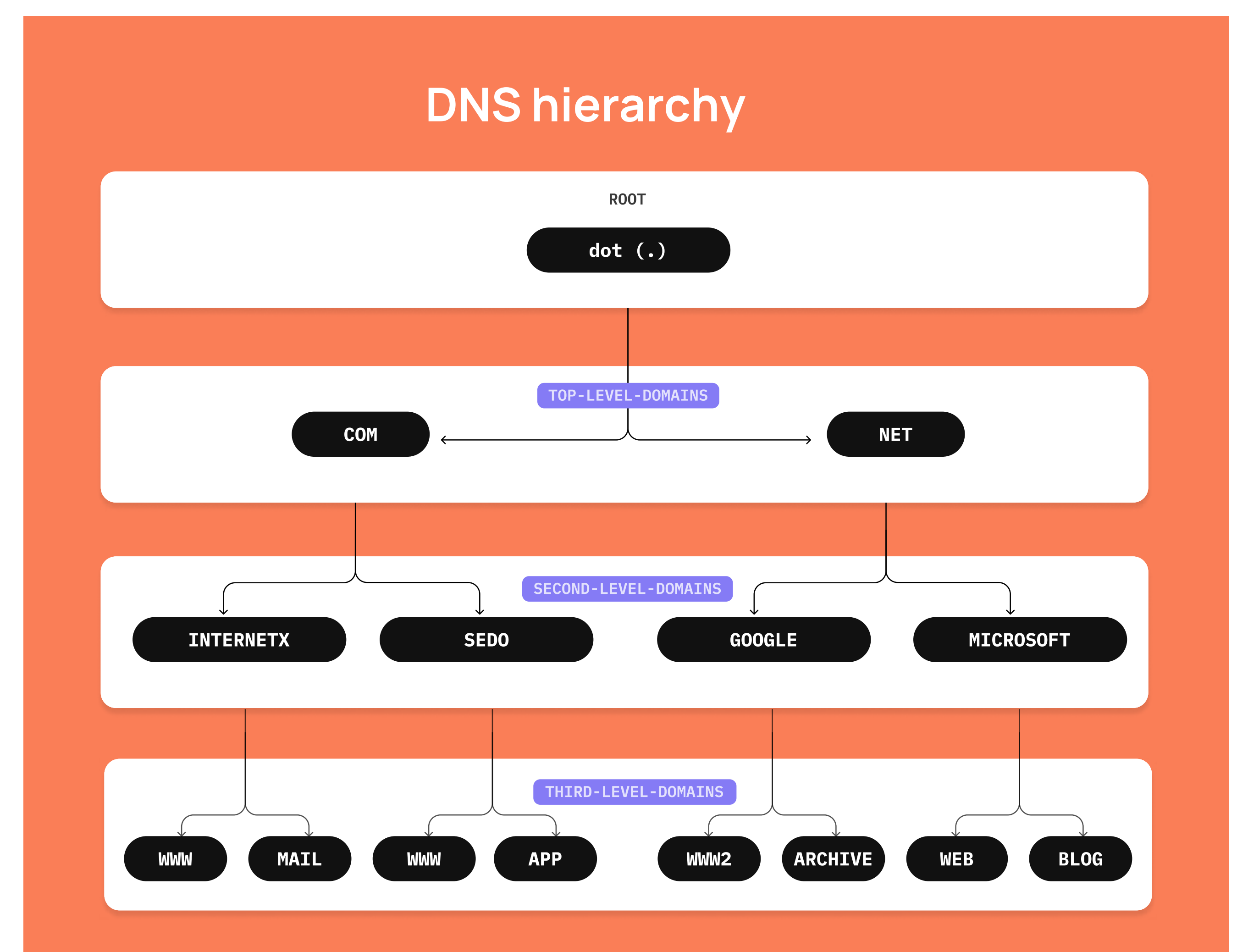
IANA coordinates the global DNS Root, IP addressing and other Internet protocol resources.

Thus, IANA manages and keeps track of all the top-level domain (TLD) allocations. One of our responsibilities involves the assessment of requests to change the operators of ccTLDs. Additionally, we are tasked with the day-to-day upkeep of the information related to the current operators.

The DNS software relies heavily on IANA's official record of TLD allocations to effectively respond to DNS queries. By having a centralized registry of TLDs, IANA ensures that DNS queries are correctly resolved and directed to the appropriate servers. This ultimately helps internet users access websites and other online resources seamlessly.

3 How do you allocate and assign IP addresses?

IANA allocates large blocks of IP addresses to five regional internet registries (RIRs) that allocate smaller blocks to regional Internet service providers (ISPs) and network providers, who then allocate individual IP addresses to their customers. Global policies have established the formulas for determining when an RIR has exhausted enough of its current allocation of numbers to require more.



Currently, IANA allocates IP addresses through two internet protocol versions, namely IPv4 and IPv6. There are two standards or "versions" of IP addresses:

- ▶ IPv4 uses 32 binary bits, allowing 4 billion unique IPv4 addresses.
- ▶ IPv6 uses 128 binary bits, allowing a larger number, at least 4 billion times the size of the IPv4 address space.

IANA exhausted its supply of IPv4 addresses in 2019 and has no more to allocate. IPv6 provides almost unlimited unique IP addresses with no risk of exhaustion.

Domain names

Management of the DNS root zone (assignments of ccTLDs and gTLDs) and other functions, such as the .int and .arpa zones.

- Root zone management
- TLDs database • .arpa registry
- .int registry • IDN practices repository

Number resources

Coordination of the global IP and AS number spaces, such as allocations made to RIRs.

- IP addresses and AS numbers
- Network abuse information

Protocol assignments

The central repository for protocol name and number registries used in many internet protocols.

- Protocol registries
- Time zone database



4 *How does IANA contribute to the stability and security of the DNS?*

The IANA functions are pivotal in improving the security and stability of critical internet infrastructure in two key areas.

1. One of the main functions of IANA is maintaining a unified namespace for the DNS, which is managed globally from a central root. This promotes interoperability by preventing fragmentation of domain names across multiple systems. Without IANA's service, the internet would not function reliably.

2. Additionally, IANA is responsible for managing the cryptographic keys that secure the root zone using [DNSSEC \(Domain Name System Security Extensions\)](#).

[DNSSEC](#) provides a mechanism to verify the authenticity of DNS data. IANA follows a highly transparent process, including "[key ceremonies](#)," to manage these cryptographic keys securely.



5 *How does IANA envision its role evolving in the future, considering the changing landscape of the internet with technologies like blockchain and the metaverse?*

As the internet landscape evolves with new technologies like blockchain and the metaverse, IANA recognizes the need to adapt and expand its role to support the community's changing needs.

IANA's core functions of managing domain names, IP addresses and protocol parameters remain crucial to ensuring the stability and interoperability of the global internet.

However, IANA also acknowledges that emerging technologies may require new standards and protocols that require authoritative record-keeping. Therefore, IANA will work closely with the broader internet standardization community to identify and address these needs and continue providing the services that the community requires while facilitating interoperability.

Ultimately, IANA's mission is to ensure that devices on the internet can communicate effectively and securely, regardless of the underlying technologies, so that the internet can continue to be a global platform for innovation and collaboration.

[Read the full interview](#) →





Whalebone, Co-Founder & CTO

► Have you ever experienced issues accessing a website due to a disruption in the internet's core protocols? One cause of such disruptions is an attack on the Domain Name System (DNS), which translates domain names into numerical IP addresses.

In the European Union (EU), most businesses rely on public DNS resolvers operated by entities outside the EU. Unfortunately, this leaves them vulnerable to cyberattacks and geopolitical incidents. Recognizing this critical vulnerability, the European Commission has come up with the [DNS4EU initiative](#) – a public DNS resolver service established within the [European Alliance for Industrial Data, Edge and Cloud](#). DNS4EU aims to provide a safer alternative for global internet access, ensuring the security and protection of Europe's digital infrastructure. Aligned with the [European cybersecurity strategy](#) from 19 February 2020, this groundbreaking initiative adheres to the latest security, data protection and privacy standards.

DNS4EU is currently under development by a consortium of companies led by the Czech cybersecurity firm Whalebone. Today, a special guest is helping us shed light on this project: Robert Šefr, the co-founder and CTO of the company. As a cybersecurity visionary, he brings a wealth of IT and security experience from his previous work at McAfee VAD Comguard, where he climbed the ranks to become the Comguard CTO.

Robert will share his invaluable insights on the significance of DNS4EU and its pivotal role in shaping Europe's digital infrastructure. This conversation promises to be both inspiring and eye-opening, giving us a glimpse into the future of European cybersecurity.

DNS4EU PROTECTS EU DIGITAL SOVEREIGNTY. “

Creating a strong and privacy-conscious DNS resolution service in Europe allows everyone to use the internet with trust.

Don't miss out on an exciting opportunity to learn more about the innovative DNS4EU and join us as we explore this fascinating project with Robert.

❶ *What are the reasons behind the EU's project to create a European DNS resolver? What are the main issues that DNS4EU aims to address?*

DNS4EU arises from the recognition that a significant number of public resolvers dominating the current market are operated by non-European entities. The European Commission now supports European companies and organizations in developing an alternative service.

i A DNS resolver is a service that translates domain names into numerical IP addresses so that users can access websites on the internet.

DNS4EU demonstrates the EU's dedication to enhancing digital security and privacy. It acts as a strong defense against external and internal risks, all while safeguarding the digital strength of the European Union. Creating a strong and privacy-conscious DNS resolution service in Europe allows European citizens, businesses and organizations to use the internet with trust. This ensures their information remains secure and their online activities stay resilient despite evolving cybersecurity risks. DNS4EU will not be developed internally

by the European Commission. Instead, the critical task has been delegated to a consortium of CERTs, academic institutions and the private sector. The commercialization of the service is encouraged by the European Commission since it is also expected that it remains sustainable without operational costs from the EU.

❷ *What are the specific objectives and aims of DNS4EU?*

The primary objective of [DNS4EU](#) is to safeguard the digital sovereignty of the EU by offering a private, safe and independent solution that empowers the region to maintain control over its online activities and protect its sensitive data from external influences.

DNS4EU has several objectives and aims that can be categorized into four distinct areas, which are as follows:

► **Create EU's digital sovereignty**
DNS4EU is committed to enhancing the EU's digital sovereignty through multiple strategic approaches:

- A European consortium will manage the service that will be based on European technologies ensuring sovereignty at multiple levels.
- DNS4EU will be built on European technologies, reinforcing the EU's independence and self-reliance in the digital realm. This emphasis on European technologies contributes to preserving sovereignty within multiple layers of the DNS infrastructure.
- DNS4EU guarantees that all user data remains securely stored within the EU space, preventing unauthorized access and safeguarding the EU's data sovereignty.

► Onboard 100 million users

The ambitious objective of onboarding 100 million users onto the internet underscores the need to go beyond relying solely on a public resolver. This goal is far beyond what public resolvers can achieve as it would require manual configuration by end-users, thus necessitating the delivery of DNS4EU via different methods. Fortunately, the project's goal of commercial sustainability can be attained through collaboration with ISPs and telcos. These collaborations can provide customers with a safe and EU-compliant solution, expanding DNS4EU's reach and propelling it toward its objective.



► Improve security

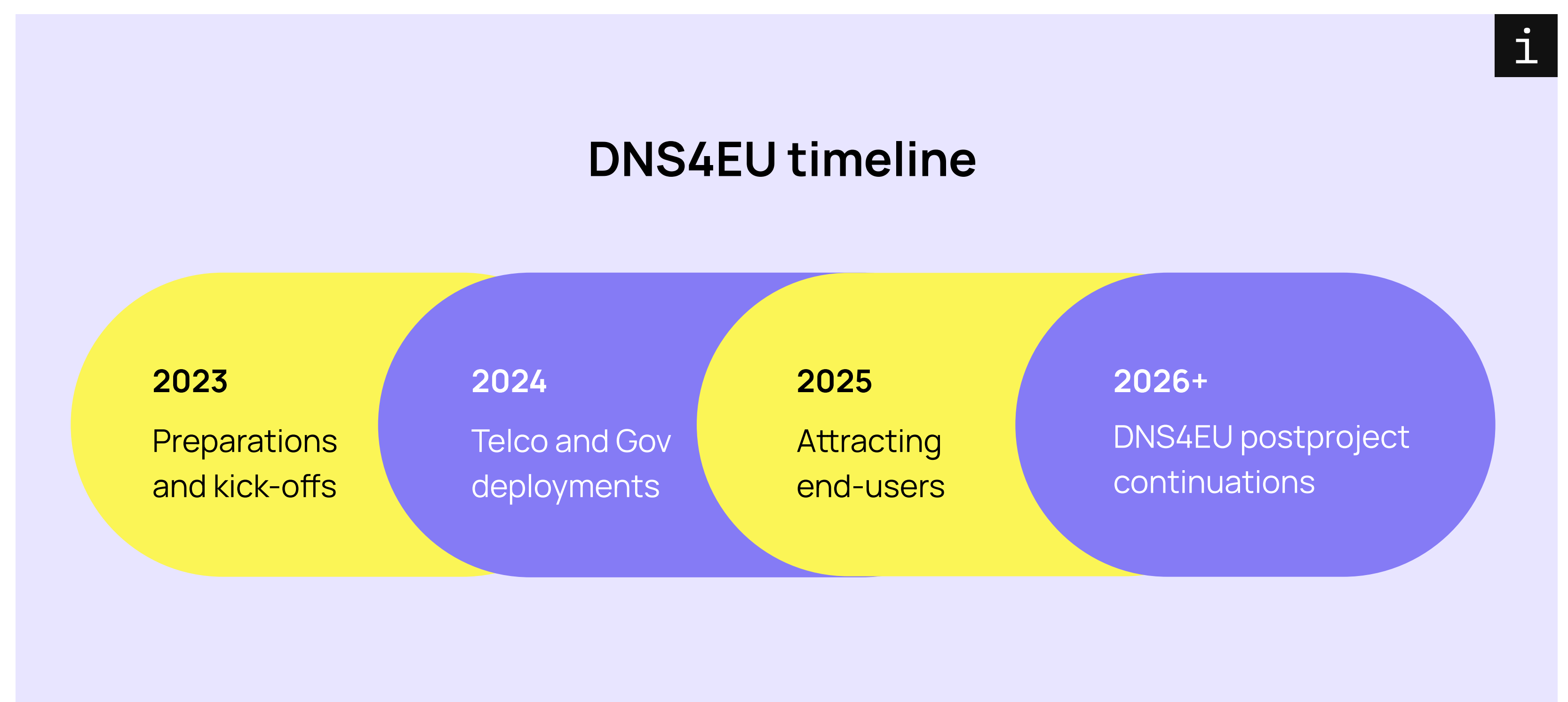
Traditional global services and security products often prove inadequate in identifying and mitigating local, state-specific online threats. In contrast, DNS4EU's dedicated focus on member states within the EU will offer exceptional protection to its citizens. DNS4EU can better identify, prevent and respond to state-specific online threats to safeguard the EU digital environment by providing a comprehensive and localized approach to online security.

③ *What level of privacy and security can users expect from DNS4EU and what measures are in place to prevent any potential tracking or monitoring of users' online behavior?*

► Enhance privacy

A key objective of DNS4EU is to prioritize and enhance the privacy of EU citizens by guaranteeing the utmost security and protection of their data. This commitment includes strict compliance with GDPR regulations and other privacy-related initiatives, ensuring that all data handling remains exclusively within the secure confines of the EU digital realm.

By maintaining this level of privacy, DNS4EU aims to cultivate greater trust among EU citizens, empowering them to confidently engage in online activities while safeguarding their sensitive information.

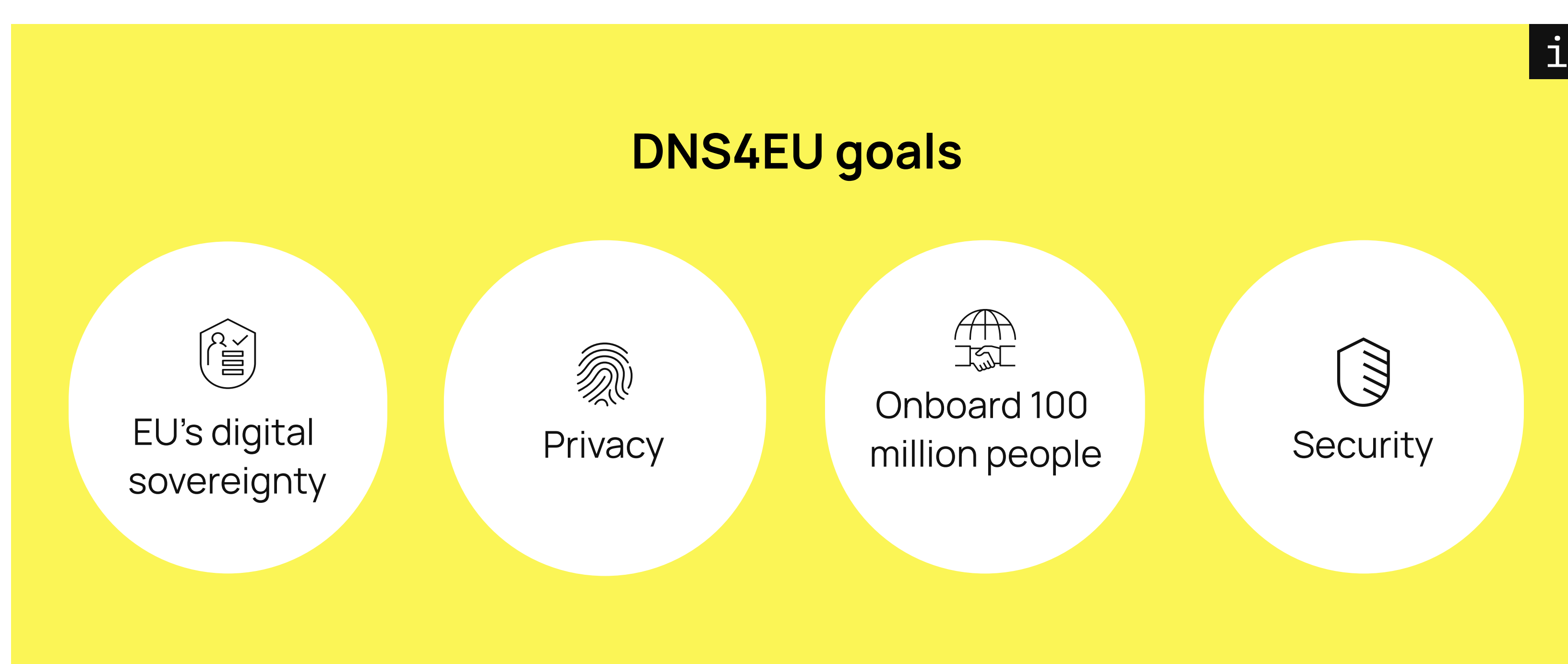


Ensuring the utmost security is our primary focus in the DNS4EU project. By implementing robust security measures, we aim to provide a DNS resolution service that proactively detects and thwarts potential threats like malware, phishing attacks and unauthorized access. Our aim is to develop a service that demonstrates resilience against DDoS attacks, ensuring the fulfillment of our commitments towards privacy and integrity.

While DDoS attacks pose a unique challenge to DNS services, we are implementing a comprehensive approach that includes proper scaling, performance optimizations, service-level DoS countermeasures and data center protection. These measures work to maximize service availability, striving for uptime as close to 100% as possible. The consortium actively discusses the privacy policy and service security to guarantee comprehensiveness and inclusivity.

Multiple viewpoints are being considered to develop a transparent and easily understandable privacy policy that aligns with best practices and user expectations. Furthermore, the public service offered by DNS4EU will prioritize anonymity.

The logs will be used solely to identify new threats within the traffic and generate aggregated reports, such as top X malicious domains. Importantly, this process will be executed without any association to the original identity of the user or their device. At the backend level, our primary focus is to ensure a thorough understanding of the data flow while minimizing the exchange of information between individual services. We prioritize the utilization of encryption wherever feasible to enhance security. Our services also undergo regular assessments to identify and address known vulnerabilities or misconfigurations. In addition, we proactively investigate potential supply chain vulnerabilities and regularly conduct external penetration tests to fortify our security measures and assess the system's resilience against possible attacks.



4 What are the main functionalities of DNS4EU that benefit governments?

Besides offering protection for thousands of organizations on the DNS level, DNS4EU also includes a solution tailored for governments and public institutions such as hospitals, schools, municipalities, banks and justice institutions with no need for installation, maintenance or user knowledge. This is an entirely different use case from just a public resolver.

We have the perfect solution on a national level, which deals with security threats such as phishing, ransomware and other security risks. The government sector focuses on multi-tenancy, allowing a central government to easily access all the logs and incident details and populate central lists of blocked or allowed domains. The architectural approach that enables the government to achieve the following is also critical – smaller institutions may redirect their DNS traffic at the perimeter from the ISP to DNS4EU. Larger institutions may, however, run their own instance of resolver within their network to gain more control and visibility. Both options are available and can be combined.

5 What is the role of telcos and ISPs in ensuring the success of the DNS4EU?

To ensure widespread access to the DNS4EU resolution across the EU, we consider telcos and ISPs essential partners.

Telcos currently handle the majority of DNS resolutions. The focus is to help them with regulatory compliance, central configuration, support for new standards and monitoring. We offer DNS4EU resolvers through telco networks and manage the complete DNS traffic.

This allows us to assist telcos in delivering exceptional quality of service and regulatory compliance while ensuring a transparent privacy policy for the end users.

Regulatory requirements are applied on the DNS traffic throughout European member states at increasingly frequent intervals and the burden of fulfilling them lies on telcos. We help keep various blocklists up to date and adequately applied and explain to the end-user why access was blocked using appropriate language, branding and context. Besides simple blocklists, many countries are introducing or considering pushing telcos to offer optional filtering for adult content and we can take this burden on ourselves and support telcos in fulfilling the requirements.

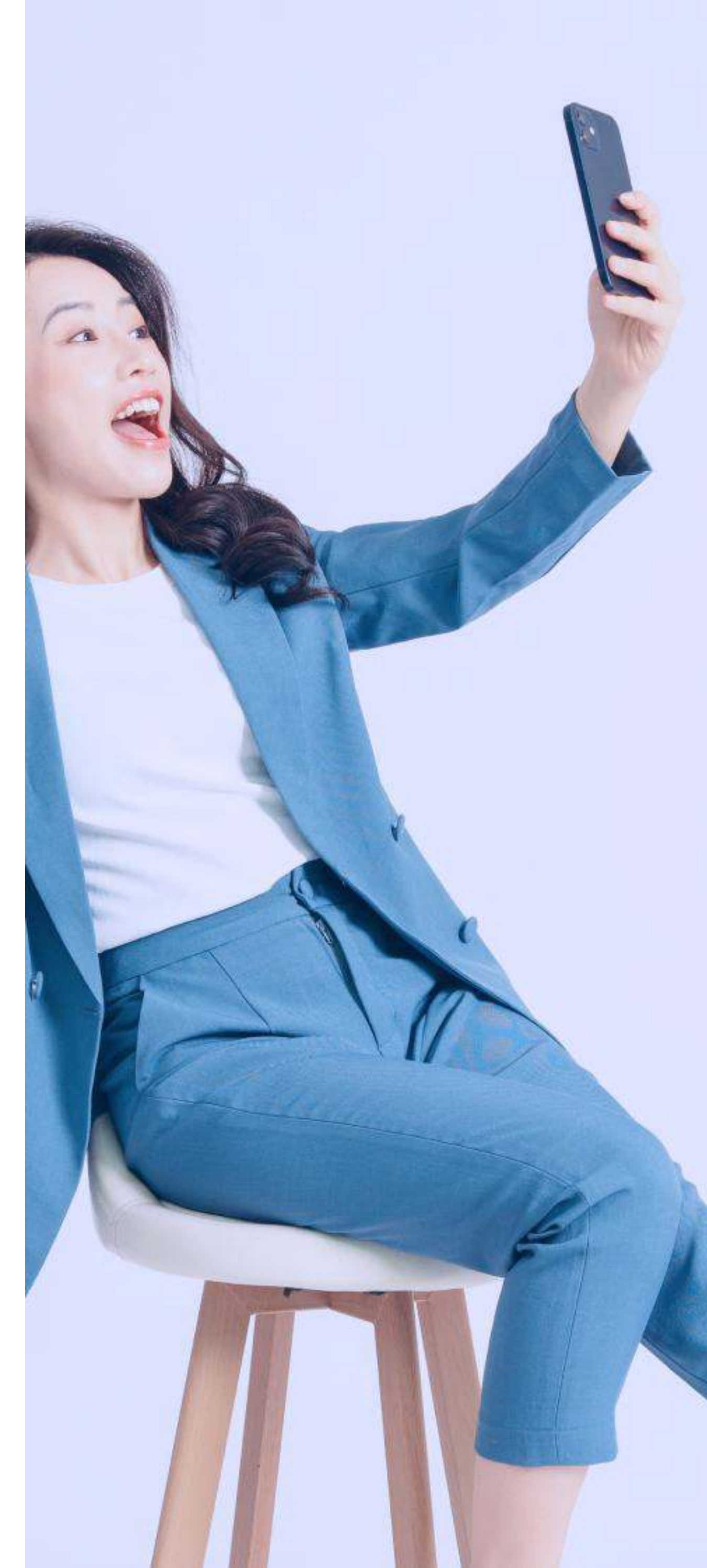
Telcos also often hesitate to introduce encrypted DNS protocols. We are ready to help them with the standard support from various networks. Experts nowadays discuss DNS over QUIC, yet many telcos still need to introduce DNS over TLS or DNS over HTTPS. We can help also with the protocol registration into the applications or operating systems and managing the certificate lifecycle.

6 Is DNS4EU going to filter some kind of content?

The public service will act following the preferences of end users. If they desire an unfiltered DNS, it will be available and the resolver will strictly follow the DNS standard without detours or blocklists.

However, we want to primarily communicate the IP address with the security filtering included, as this security layer should be a part of everyone's digital life. No regulatory blocklist will be implemented, as such lists do not impact DNS services; instead, they pertain to internet service providers.

The offering for telcos and ISPs will indeed include support for regional blocklists. That is legislation that telcos cannot avoid and which they have to introduce through any DNS technology of their choice, whether DNS4EU or other. As far as we know, no blocklists would recall any political, religious or similar censorship across the EU.

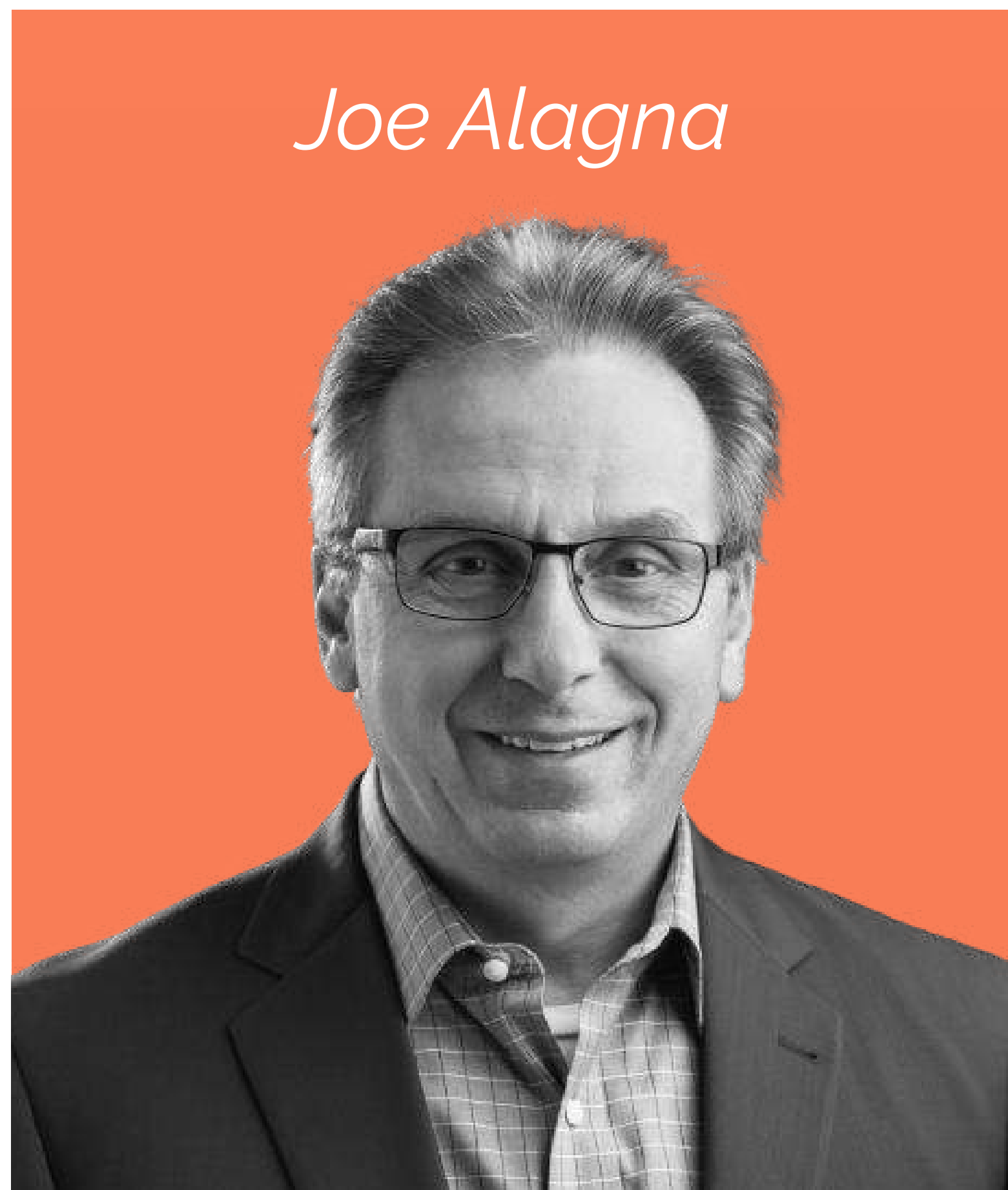


i

DNS4EU for telcos

Telcos	End users
<ul style="list-style-type: none"> • On-premise DNS resolvers • National regulatory compliance • DNS standards support and compliance • Telco grade resolver incl. API, monitoring, logging, troubleshooting and integration features 	<ul style="list-style-type: none"> • Lower latency than public resolvers • Transparent privacy • Optional protective features

[Read the full interview →](#)



Joe Alagna

it.com, Director Business Development

► In today's dynamic digital landscape, domain names are pivotal in shaping online identities. While we are all familiar with the predominant gTLD .com, a new player has entered the game, offering a fresh perspective on domain registration: it.com, technically a third-level domain. With its unique syntax, it.com creates memorable addresses for brands, organizations and individuals.

But how exactly does a third-level domain like it.com work? To answer that question and unravel the intricate nuances of it.com, we had the pleasure of interviewing a seasoned professional in the domain industry: Joe Alagna, Director of Sales at the it.com registry. With over 20 years of experience working with domains and having served in fundamental roles at big players in the industry, Joe's insights are valuable for professionals and enthusiasts alike.

As our engaging conversation with Joe unfolds, we'll explore it.com's origin, features and growth. We'll also discuss how its versatility can benefit businesses and individuals looking to style their online presence.

Buckle up and get ready for our tech-savvy discussion with Joe Alagna – a journey that inspires and defines the ever-evolving domain industry.

THE WORLD LOVES A DOMAIN ENDING IN .COM!

Discover the pioneering innovation of the it.com registry, where novelty and technology intersect in the fascinating expanse of the namespace.

❶ *it.com is a new domain registry: Where does the story start? What are the notable milestones and achievements the registry has accomplished so far?*

Setting up the it.com registry was the idea of our CEO, Andrey Insarov. Andrey is the founder and CEO of an ongoing IT company called Intis Telecom. The company has an annual turnover of \$40M and provides short messaging services for some of the largest telecom companies from all over the world. In 2021, Andrey purchased the domain name it.com, initially as a way to shorten and simplify his domain name. But he soon realized that it.com could benefit many more people and companies than himself. So, he decided to get ICANN accredited and build a registry offering [it.com](#) to other IT companies.

I came on board in 2022 and by the time I joined the company, the registry was already a work in progress. Had they not built those systems already, I might have advised them to outsource the registry, but it looked really good and reminded me of my early days at CentralNic. Relying on our own registry system, we spent the last quarter of 2022 developing our legal and policy issues. We onboarded some essential brand management registrars and launched our [sunrise](#) in January 2023. We got hundreds of registrations during the launch and brought on a majority of the largest IT companies in the world, commonly described as "FAAMG" companies, in the US stock market. They registered their [it.com](#) domains for brand protection purposes.

Since mid-February 2023, we've been spending our time building our channel. We've brought on over 20 significant registrars, including [InterNetX](#) and our goal is to have ten thousand domains under management by the end of 2023!

❷ *What sets the nature of it.com apart from other TLDs?*

First, I must point out that when you refer to it.com domains, they are most appropriately called "third-level domains" rather than top-level domains (TLDs). We like to refer to our domain as an "extension," a "suffix" or even an "ending" rather than a TLD. This is to reduce confusion and to be truthful about what our product actually is.

► A third-level domain is an additional part of a domain name that extends an existing second-level domain by another layer. It precedes the second-level domain and the top-level domain in the domain hierarchy. Third-level domains are commonly used to organize content, services or region-specific resources within a larger domain structure.



3 *What is the strategy behind registering it.com domain names and their target audience?*

The term "IT" has a dual meaning in the context of the domain name it.com. While "IT" commonly stands for Information Technology, it also signifies the word "it" in everyday language. Acquiring an it.com domain can evoke the idea of possessing "it" – a desirable and intangible quality encompassing charisma, confidence, charm and overall appeal. Thus, it.com represents more than just a tech-related domain name; it embodies a sense of completeness or "having it all" for its registrant.

Many domainers are registering it.com domains as a call to action. These include domains like do.it.com and buy.it.com. These websites have yet to be developed, but we hope to see some exciting things from these domains. Our primary targets are the IT industry and, of course, Italians. These are the most intuitive markets we've identified in our domains. Our suffix gives them a way to get short, meaningful strings and helps them identify with what they do or are about. It's also meaningful that our suffix ends in .com. The world loves a domain ending in .com!

4 *What are your day-to-day responsibilities as the Director of Sales at it.com? Also, how do your tasks align with the company's overall strategic goals?*

As the Director of Sales at it.com, a crucial part of my role involves managing our strategic direction. This necessitates regular analysis of market trends, staying updated on any changes within our industry and adjusting our marketing strategies accordingly.

Security: Under the TRUST framework, security involves maintaining robust measures to protect our registry not only against cyber threats but also from rules and policies like GDPR and NIS2, especially in dealing with disputes, fraud, spam, and other malpractices. It implies:

- Signing zone files to provide registrants with a secure way to build their online presence.
- Cybercrime analytics using modern tools to combat domain abuse.
- Using the best security tools, firewalls and DNS security expertise to keep the systems safe.
- Strengthening server security: servers must be safeguarded at all levels.
- Partnering with global authorities to tackle spam, phishing and other types of DNS abuse.
- Education for staff: Ensuring an informed workforce through continued training.

Our company structure is highly collaborative. Consequently, I work closely with colleagues to align our sales objectives with the organization's broader goals.

I see myself more as a coach and advisor, using my past experiences at other companies to help us successfully get through these beginning stages. I certainly couldn't do this without the unwavering support of our CEO. He is determined to see it.com through to long-term success and has the resources necessary to make it happen.

i



5 *How does it.com ensure the security of its domains and protect against potential threats?*

Security is always a personal responsibility but our registry provides all the tools and protections needed to help people secure their online presence.

We have developed all the standard policies to prevent trademark infringement and abuse of domains. We have a take-down policy and a zero-tolerance for malware and abuse. The root of the it.com zone is signed so that registrants can protect their domains using SSL with the assurance that there is a complete chain of security from their third-level domain down to the .com root.

We're also part of the PSL (Public Suffixes List), which allows browsers to differentiate cookies from one subdomain to another. The PSL was a voluntary effort slowly being migrated towards management by ICANN.

6 *How does it.com ensure the security of its domains and protect against potential threats?*

Security is always a personal responsibility but our registry provides all the tools and protections needed to help people secure their online presence.

We have developed all the standard policies to prevent trademark infringement and abuse of domains. We have a take-down policy and a zero-tolerance for malware and abuse. The root of the it.com zone is signed so that registrants can protect their domains using SSL with the assurance that there is a complete chain of security from their third-level domain down to the .com root. We're also part of the PSL (Public Suffixes List), which allows browsers to differentiate cookies from one subdomain to another.

The PSL was a voluntary effort slowly being migrated towards management by ICANN.



7 *Are there any specific niches that have seen success or benefits from using it.com?*

Although we didn't expect it, our earliest successes have come from the Italian market. We were fortunate to have hired Alessandro Baruffi, who spent many years working for Tucows. Alessandro has an excellent reputation in the Italian domain market and has helped us bring many Italian registrars and resellers on board. We've done several events in Italy and are finding great acceptance of the it.com domain there.

Registrants of .it domains are finding significant benefits in registering the it.com extension because, by habit, many of their visitors from the US and other countries add .com to their domain when typing it into their browser. This is called traffic leakage and bears a significant unknown cost to .it registrants. By owning and redirecting their it.com domain to their .it domain, these registrants eliminate that online traffic leakage.



8 *What future developments or plans does it.com have for the registry and its customers?*

2022 was the year we developed our registry infrastructure and policy.

2023 has been the year of growing our channel. We spent much time and effort recruiting and evangelizing domain name registrars.

In 2024, we aim to continue and enhance that effort by reaching out to the global IT community. There are many technical and public perceptions for us to overcome, but we have already achieved significant breakthroughs on both fronts and are continuing to move forward.

[Read the full interview](#) →



Sophie Pieck

Sedo, Director Business Development

► The domain aftermarket serves as the primary playing field for most domain experts. This market is where domains are bought, sold, parked and auctioned. However, its impact extends beyond these simple transactions. Significantly, it influences the online presence and branding of major organizations, entrepreneurs and individual creatives. In essence, the domain aftermarket plays a crucial role in shaping the digital identities of businesses and individuals alike. In the domain aftermarket, one organization distinguishes itself as a leading global player: [Sedo](#). With its unmatched expertise and broad range of services like the SedoMLS integrated into AutoDNS, Sedo has firmly established its place in the rapidly growing and competitive marketplace of domain names.

And who would be better equipped to enlighten us on the domain aftermarket than Sophie Pieck from Sedo? With an impressive career that spans various geographies and industries, Sophie's journey in the domain aftermarket is nothing short of remarkable.

Before joining Sedo, Sophie worked in the trade show industry. She was instrumental in internationalizing local trade shows and organizing satellite events in markets across China, Russia, Turkey and the US. Sophie's tenure at Sedo took off as a Country Manager for France and Italy, providing her with a rich blend of experiences dealing with domain investors and buyers from these markets. Her role expanded as she courted opportunities in the Indian market, fostering growth and building lasting partnerships. Today, as Director of Business Development since 2017, Sophie oversees Sedo's B2B relationships with registrars, registries and various domain service providers.

WHERE DOMAINS TRANSFORM INTO DIGITAL GOLD!



Venture into the bustling bazaar of the domain aftermarket:

This conversation promises to be an exciting deep dive into the realm of domain aftermarket and Sedo's pivotal role in shaping it, seen through the experienced lens of Sophie Pieck. As we turn the pages of her professional diary, we uncover valuable insights about this thriving segment of the domain industry and its ever-evolving dynamics. Join us on this journey!

❶ *In today's digital landscape, domains have become a valuable digital asset. What makes them so valuable?*

Domains are considered digital assets because they can be bought, sold and used as a form of online property. There are several reasons why a domain is valuable for companies, brands and investors alike:

- Trust and credibility
- Branding and visibility
- SEO benefits

Overall, they have a competitive advantage that tremendously impacts brands. The special thing about domains, compared with conventional assets such as shares, real estate, art, and others, is that each domain is unique and cannot be repro reproduced at will.

Even if there are dozens of brands that would like to use music.com, there can only be one company that owns it! This increases the value of domains enormously.

❷ *Working at Sedo, you must get incredible insights into the domain aftermarket. What are the unique opportunities this industry segment offers to businesses today?*

All short, memorable domains, above all under legacy TLDs, are already taken. For businesses, reaching out to aftermarket platforms such as Sedo allows them to find the domain they want for their brand or marketing campaign. With almost 25 years of experience in the industry, Sedo is a trustworthy partner that can help businesses, even when the domain is not for sale, for example by reaching out to the current owner and helping to negotiate the best possible price for the domain anonymously.

Access to the right domain is crucial for any business, regardless of brand size. While the aftermarket gives access to end users to find the domain they are looking for, it also offers a wide range of opportunities for companies within the domain industry: registrars and registries, as well as website-building services, are getting access to features or services, such as [Sedo's brokerage service](#), that are helping them to grow their own business, increase their revenue and keep a high level of customer retention. Connecting primary market companies with the aftermarket is a win-win situation for the whole network.



3 What are some of the critical factors that determine the value or price of a domain in the aftermarket?

There is a guiding principle similar to the real estate market: what location is to the real estate market, and what shortness is to domains.

As a longtime provider of domain appraisals, we have found that the key contributing factors to the value or price of a domain on the aftermarket are as follows:

Domain length and memorability:

short, memorable domain names often fetch higher prices due to familiarity and ease of use. Memorable domains are more likely to attract direct inbound traffic. While this naturally generated traffic was critical years ago, it is now minimized by the immense use of search engines. Search engines now play a major role in determining who is at the top of the search results. Nevertheless, a short domain has advantages that can save a lot of money in a company's marketing budget. For example, with TV advertising, every second costs money. The shorter the domain name, the lower the advertising expenditure.

Domain extension and its combination with the keyword:

Well-established endings such as .com, .net, .org enjoy a high level of awareness and wide usage and have therefore been the almost undisputed favorites of customers for years. I say almost because there are, of course, also endings that suddenly stand out due to social events and developments. These include .ai or .io, for example, endings that go hand in hand with technological progress.

Other influential factors include, to name a few:

The popularity of keywords, an established online presence and authority, whether domains align with popular trends, technologies or industries, similar sales data, existing traffic or revenue streams and many more.

4 What are the major trends and challenges in the domain aftermarket that businesses and domain resellers should be aware of?

The most influential trends domain resellers should keep an eye on in the coming months are AI, renewable energies

and voice search. Domains or endings related to these topics will be in greater demand.

Those who want to continue to focus on short and descriptive domains in combination with the most common endings are always pursuing a good strategy. Topics such as crypto or NFTs will be less relevant. This brings us to the challenges. There are always short-lived trends, such as investing in domains with the keyword "meta," which then cool down again after a certain period of time. In the worst-case scenario, you can be left sitting on your portfolio if you focus too much on temporary trends.

We recommend securing a few assets first and then testing how demand develops. Anyone involved in the domain name business needs to have perseverance. It is not unusual to sell a domain only after eight years. But the profit margin is very high.

From a business perspective, the availability of good domains could become problematic. More and more brands are getting their desired domain for the reasons mentioned above and are spending more in order to be truly distinctive. The more these perfect ultra-premium domains are in use, the more difficult it will be for other brands to get their hands on them.

Geopolitical events and economic influences pose a further challenge. This has been demonstrated in recent years, which brought several crises. People did not have ready access to liquid financial resources and higher interest rates meant getting money or investing large sums was more challenging. This has had an impact on the purchasing power of domains. We will see how this develops in 2024.

AutoDNS meets Sedo Get the best of both worlds.

The screenshot displays the AutoDNS interface. At the top, there is a red header with the AutoDNS logo and a "Start selling" button. Below the header, a white box titled "Boost your domain sales with SedoMLS" lists three benefits: "thousands of potential buyers worldwide", "triple your sales potential", and "receive your sales revenues as fast as possible". Below this, there are navigation buttons for "Marketplace", "Bulkselling", and "DNSSEC". The main section is titled "Domain portfolio" and shows a list of domains for sale:

Domain	Action
earnmoney.com	Sell \$
moneymaker.de	Sell \$
earnmoney.ai	Sell \$
makemoney.xyz	Sell \$

5 *How do aftermarket integrations, such as SedoMLS, aid registrars in remaining competitive and benefit their customers regarding domain access, revenue generation and service offerings?*

Aftermarket integrations, such as SedoMLS, give both end users and resellers easy access to already-registered domains. With this integration, you can look for any domain listed for sale on Sedo directly on your registrar's website. InterNetX, for instance, has had an aftermarket integration with Sedo through AutoDNS since the beginning. Users can search for aftermarket domains directly through AutoDNS and place their

domain in the basket. It's just as easy as that. And what's more, users can also list their domains for sale on Sedo through AutoDNS. Using the aftermarket integration of SedoMLS allows registrars to remain competitive by generating new revenue streams and satisfying the needs of their customers.

Two out of three customers who buy an aftermarket domain will not only register their domain for several years, but purchase value-added services offered by their registrar. By allowing customers to list their domains for sale and monetize them on the aftermarket, registrars can increase their renewal rate.



6 *How have you seen the domain aftermarket evolve during your tenure at Sedo and what is your vision for the future of the domain aftermarket?*

I started working at Sedo during an exciting time for the industry, as it was a period when hundreds of new gTLDs had been launched and entered the domain landscape. During that time, the industry started increasing interest in promoting those new premium domains in the secondary market. Over the past ten years, there has been a shift where both registries and registrars understood the increasing value of entering the secondary market by listing their inventory on Sedo or offering Sedo's domain inventory to their end-users.

Our inventory, with 24 million domains for sale, has been growing year over year. Such has been the demand for premium domains! Especially during the pandemic, we saw a significant increase in aftermarket sales for highly valuable domain names.

But users can also find more affordable domains on the aftermarket as Sedo has been extending its partnerships with businesses listing their expiring domains for sale.

Moving forward, I believe the domain aftermarket and primary market will merge more and more. Registrar businesses and other domain service providers understand the importance of keeping their customers, being able to offer them a solution for their domain needs, and avoiding "dead-end searches."

Aftermarkets such as Sedo help with that, which is why more and more registrars are integrating our aftermarket services. Sedo is helping close this gap and help registrars or other providers offer the best service to their customers.

So many users are looking for a great domain that fits their needs and Sedo will keep helping them get the domain they are looking for.

[Read the full interview →](#)



Giovane Moura

SIDN Labs, Data scientist

► In technology, the science behind operations is rooted in academic settings. Breakthrough developments aren't just theorized there. They are tested, adopted and eventually shared with the general audience. DNS is no exception. Today, we're thrilled to be talking with an expert who combines two realms that often seem to be worlds apart: the technical DNS industry and the academic sphere.

It's a pleasure to introduce Giovane Moura, a data scientist at SIDN Labs and an assistant professor specializing in cybersecurity at Delft University of Technology (TU Delft). Giovane works with SIDN Labs, the research hub of SIDN, the registry operator of .nl, the ccTLD of the Netherlands.

Giovane finds himself at the frontline of DNS operations advancements but doesn't stop there. In the halls of TU Delft, one of the leading universities in technology worldwide, he rigorously applies academic principles to the security, performance and stability of networked systems.

Our discussion will take a deep dive into Giovane's wide-ranging research, covering critical areas like Anycast, DNS engineering, DDoS attacks and DNS security – topics in which he is steeped in knowledge.

We'll engage with the academic perspective on DNS, uncovering important insights on security concerns and vulnerabilities. You should keep your notebook at hand because Giovane will also drop some invaluable DNS security tips, informed by years of research and practical expertise.

DOMAIN INDUSTRY MEETS DNS RESEARCH.



Scholarly insights meet real-world DNS challenges. Let's explore the hidden corners of the DNS labyrinth.

Brace yourselves for an engaging conversation with Giovane Moura in which academia meets DNS industry practice!

❶ *What is the present state of research in the field of DNS? Are there any current hot topics?*

DNS is a 26-year-old protocol that has continued evolving since its inception. It includes a suite of protocols, a distributed database system and a client-server architecture at its core. The system is integrated with extensive routing methodologies, particularly *Anycast*, and encompasses a significant focus on security aspects such as phishing and spam prevention. Governance is another crucial facet of DNS.

With over 2000 pages of insightful documentation, often referred to as the DNS camel, it's fair to say that DNS remains a bustling research field across all of these fronts.

► **Regarding DNSSEC, a considerable amount of research is being conducted in the context of post-quantum computing. The key question emerging in this field is: What implications will the advent of quantum computers, capable of quickly deciphering most DNSSEC algorithms, have for the security integrity of the DNS infrastructure?**

► **Within the authoritative side, experts are diligently focusing on the automatic deployment of Anycast services to meet the demands of growing service needs effectively.**

► **Regarding zone contents, there's an ongoing, complex dance akin to a cat-mouse game concerning abusive domains. As soon as a malicious pattern is identified, offenders usually modify their strategy, instigating a continuous cycle of challenge and response.**

► **In recent years, numerous standards have emerged focusing on encrypting DNS traffic. Notably, DNSSEC primarily safeguards integrity but doesn't address confidentiality. Consequently, we now have new IETF standards like - DNS over TLS (DoT), DNS over HTTPS (DoH), and DNS over Quic (DoQ) to tackle confidentiality issues. While these are formally established standards, their actual adoption presents an entirely different challenge.**

Therefore, we need comprehensive measurement studies to shed light on the performance and prevalence of these protocols in contemporary networks.

► **DNS centralization is another issue that academia and the DNS industry focus on. We are witnessing a significant surge in traffic gravitating towards large cloud service providers. This trend concentrates power and control in the hands of these top providers and potentially compromises the resilience of the internet infrastructure. It is a concern that warrants attention from all DNS stakeholders to ensure a fair and stable digital environment.**

2 *At the end of 2021, you disclosed the tsuNAME vulnerability. What does this DNS security flaw entail?*

The vulnerability, which we named tsuNAME, involved clients and recursive resolvers endlessly sending queries to authoritative servers. If a record X points to Y, and Y points back to X, it creates a loop. For this looping behavior to begin, a resolver or client must identify a DNS zone loop within zone files located on different servers. Upon detecting this, some resolvers won't simply stop querying: They will instead start looping and sending queries non-stop, hoping each query will return a different answer. When exploited deliberately, this issue could overwhelm and incapacitate authoritative servers. As a result, it would make entire DNS zones inaccessible.

At its first stage, our research showed that the ccTLD .nz suffered a 50% traffic increase because of its vulnerability and that Google Public DNS (GDNS) and Cisco Open DNS could be steered to send many DNS queries to authoritative DNS servers this way, which caused a 10-fold traffic increase for an EU-based operator.

The tsuNAME disclosure process encompassed early notification to domain operators, managing stressful responses, navigating vendor responsiveness and navigating through an eight-month path from the initial discovery to a final public disclosure. To prevent tsuNAME from being used for DDoS, we worked closely with vendors and operators and Google and OpenDNS promptly fixed their software.

In the meantime, the RFC 9520 published in December 2023 proposes that resolvers cache such cycling records so they no longer loop.

About SIDN

▶ SIDN is not a commercial enterprise. We are professional and businesslike, but with a view to maximising the value we create for the community and economy of the Netherlands. We use the earnings from new products to reinforce the position of the .nl domain, to promote growth in the field of cybersecurity and online identity, and to invest in the Dutch and international internet communities. Those goals are pursued through the operations of SIDN Labs and SIDN Fund, for example.

3 *What technical strategies can DNS operators and developers employ to bolster the defenses of DNS against DDoS attacks?*

Implementing replication is crucial to defending DNS against DDoS attacks. This means setting up multiple authoritative servers and using IP Anycast within these servers, enabling them to be announced

from various locations – a technique often called over-provisioning. Over-provisioning via IP Anycast provides a robust defense against DDoS attacks.

By utilizing multiple authoritative servers, traffic can be evenly distributed, reducing the risk of any single server becoming overwhelmed. Additionally, the ability to announce these servers from multiple geographical locations enhances redundancy and resilience, ensuring continuous availability and performance, even if an attack targets some servers.

Ultimately, this technique improves the capacity of DNS infrastructure to absorb large volumes of traffic and mitigate the potential impacts of DDoS attacks.

The Border Gateway Protocol (BGP) is a powerful defense against DDoS attacks which enables authoritative operators to control network traffic strategically.

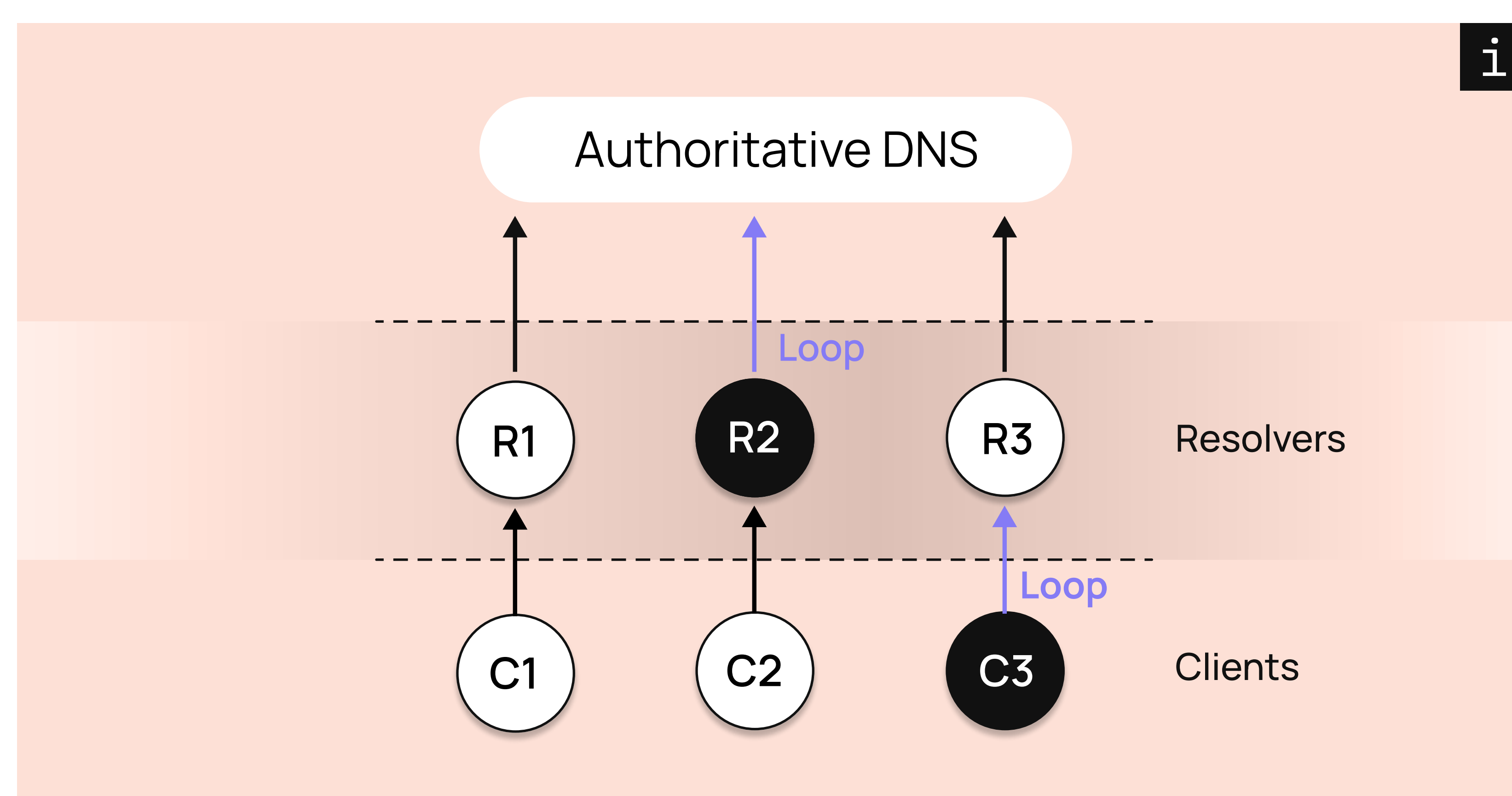
By adjusting BGP configurations, operators can lead malicious traffic away from target servers and towards locations with the capacity to handle it or even to a sinkhole that absorbs and neutralizes the attack.

We outlined this step in RFC9199. This ability to dynamically reroute traffic protects the DNS infrastructure and minimizes service disruptions during DDoS events.

Additionally, assigning long Time To Live (TTL) values to records can be protective. The TTL value in DNS records can aid in mitigating DDoS attacks through its control over how often DNS information is updated. A shorter TTL provides more regular updates, reducing the window of opportunity for attackers to redirect traffic to illegitimate servers.

Conversely, a longer TTL can be set once a threat has passed to reduce unnecessary network load. Thus, properly managing TTL values provides a dynamic mechanism for responding to and recovering from DDoS attacks.

These strategies shield user operators from large-scale DDoS attacks and offer resilience similar to that observed in root DNS servers.



4 *How can authoritative DNS server operators enhance their service offerings? Are there any specific factors they should consider or best practices they should adopt?*

If authoritative DNS server operators aim to minimize latency, the initial step would be to gauge latency from their clients using **DNS over TCP** traffic. This method enables the identification of clients experiencing poor performance, creating an opportunity to optimize their experience. Moreover, this approach is cost-effective and simple to implement. For resilience, then we are talking about replication. Anycast is an option for large operators, but it has associated costs.

5 *How does the surge in cloud computing and the expanding utilization of microservices influence DNS research and infrastructure? What potential challenges do these trends present?*

The dominance of a few key players, in particular big US tech companies, has resulted in a significant concentration of web traffic. Interestingly, this shift has had unexpected benefits. For instance, when Google activated query name minimization on its public DNS, it instantaneously impacted millions of users.

Operating servers on the cloud can offer DNS operators considerable ease as it allows them to deploy new instances as and when traffic demands increase. Yet,

What is an authoritative DNS server operator?

► An authoritative DNS server operator manages the servers containing authoritative information about domain names within a specific zone. These operators are responsible for providing accurate DNS name resolution for their domains. As the definitive source of domain information, authoritative DNS servers ensure that clients receive the correct IP addresses when accessing websites, thereby easing internet navigation.

we should heed the wise words of Bruce Schneier, reminding us that the cloud is essentially 'someone else's computer.' Research will also have to follow this tendency; the performance of large DNS providers will become increasingly important if this trend continues.

6 *How do you see DNS evolving in the next 5-10 years?*

Drawing from past trends, we can assert with confidence that DNS will continue to evolve, just as it has consistently done over the past 26 years.

I anticipate the increased use of artificial intelligence (AI) and machine learning

(ML) in DNS. Both AI and ML have the potential to enhance the security of DNS by efficiently identifying and blocking malicious traffic. They could also streamline DNS performance by predicatively analyzing user behavior and responsively adjusting DNS responses.

For instance, should we initiate a new server in Anycast location X in response to rising traffic? As the costs related to computing and storage continue to decline, implementing ML as a method to bolster both operations and security will become increasingly cheaper.

Key improvement factors for authoritative DNS server operators

1 Reducing latency: Implementing measures such as GeoDNS, Edge DNS servers or CDNs to improve response times.

2 Resiliency: Building redundancies, like deploying multiple servers or employing IP Anycast, to protect against potential failures or attacks.

3 Security: Implementing DNSSEC and improving DDoS mitigation techniques to ensure the safety of the DNS information.

4 Scalability: Design systems to handle growth and increased traffic demand effectively without sacrificing performance.

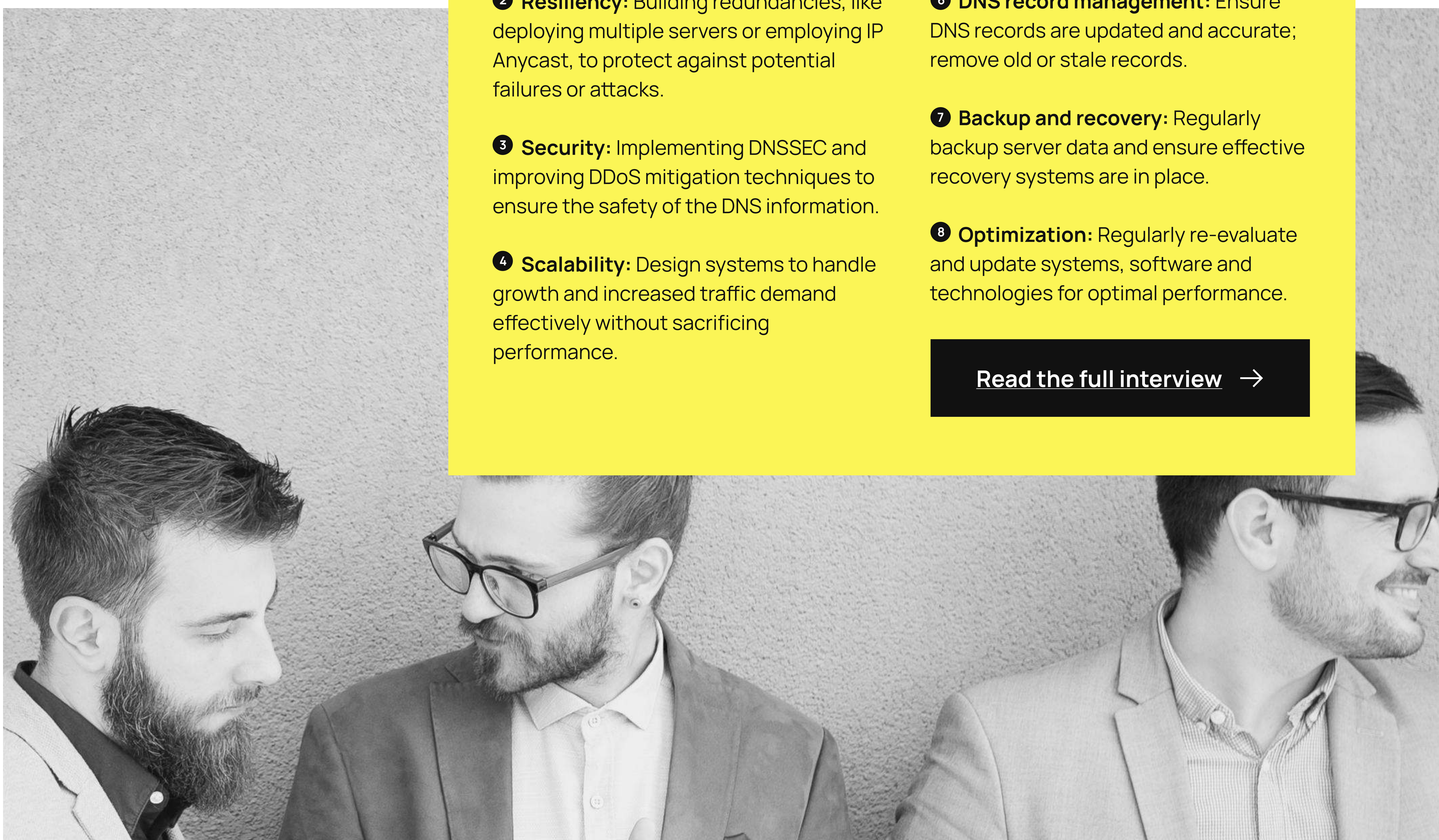
5 Monitor & analysis: Monitor server performance, latency and traffic patterns; analyze logs for anomalies or issues needing attention.

6 DNS record management: Ensure DNS records are updated and accurate; remove old or stale records.

7 Backup and recovery: Regularly backup server data and ensure effective recovery systems are in place.

8 Optimization: Regularly re-evaluate and update systems, software and technologies for optimal performance.

[Read the full interview](#) →





Polina Malaya

CENTR, Policy Director

► Policy-making and internet governance are pivotal in the domain industry. They determine how we navigate and ensure a certain level of security and interoperability. At the heart of Europe's digital space, the Council of European National Top-Level Domain Registries (CENTR) plays a crucial role in influencing policies that resonate across the continent's online infrastructure.

Today, we're thrilled to welcome Polina Malaja, the driving force behind CENTR's policy direction, where her expertise in international human rights and intellectual property law informs her advocacy for the delicate balance between technological progress and fundamental rights.

Join us as Polina delves into the complexities of digital space governance. Don't miss her profound insights—tune in to the fascinating dialogue ahead.



POLICIES ARE SHAPING THE DOMAIN INDUSTRY

Venture into the nexus of European policy & digital identity with our deep dive into ccTLD registries + their role in shaping the internet.

❶ **What does it mean to be the Policy Director at CENTR? What inspired your path into policy-making within the domain industry?**

As the Policy Director at CENTR, my primary responsibility is to spearhead CENTR's policy initiatives that impact European ccTLDs, both on a European and global scale. This involves pinpointing the issues that hold the most significance for European ccTLDs and representing CENTR's members in dialogues with policymakers and other stakeholders.

CENTR, the association of European ccTLD registries, such as .de for Germany or .si for Slovenia, aims to foster and contribute to developing high standards and best practices among ccTLD registries. The association comprises 51 full and 8 associate members, accounting for over 80% of all registered domain names globally. CENTR serves as a platform for discussing policy matters affecting ccTLD registries and acts as a liaison to internet governing bodies and other organizations involved in digital policy. It champions the interests of ccTLDs and advocates for them.

My journey in the DNS ecosystem began as a natural progression from my interest in free and open internet and the technologies that support it. As a human rights lawyer, I'm intrigued by the intersection of technology and human rights and the role that critical internet infrastructure, like the DNS, plays in our ability to exercise our fundamental rights. At CENTR, we don't just represent industry interests: We advocate for the technical community dedicated to preserving a free and open internet, with people's needs and rights at the heart of the discussion.

❷ **What do you consider to be the most critical challenge we currently face in internet governance?**

As we draw closer to the World Summit on the Information Society (WSIS+20) review, an intergovernmental process set to determine in 2025 whether the multistakeholder model for internet governance is still effective, it's crucial to underscore the achievements of the global multistakeholder model that has made the internet an essential part of our modern information society.

These accomplishments include technical interoperability, infrastructure based on open standards and decentralized solutions, and the ongoing stability and resilience of the global internet amidst wars, geopolitical tensions, and pandemics. The multistakeholder model is often overlooked in these debates. Undeniably, emerging challenges like the rise of gatekeepers and AI have shifted the focus towards other issues that need to be addressed when discussing the future of the internet.

However, it's vital to remember that the technical operation of the global internet, rooted in multistakeholder processes, enabled the human-facing web to evolve through various stages of its development. At the same time, the technology that powered this transformation remained open, free, scalable, and reliable. Without the support of all stakeholders, including governments, in the multistakeholder model, the future of one open global internet is at risk.

3 What changes do you foresee in TLD policies across Europe in the near future?

European ccTLDs are closely rooted in their national countries and are primarily subject to national (and, in the case of the European Union, regional) legislation. Consequently, policy-making within the realm of TLD administration—covering aspects like domain name registration policy, domain use policy, privacy policy, etc.—is shaped mainly by modifications in national and regional legislation.

Some of the most notable examples that have or will have a significant impact on TLD policies in Europe come from EU legislative initiatives, such as the GDPR, Consumer Protection Cooperation Regulation, Digital Services Act, [NIS2 Directive](#), e-Evidence Regulation and Geographical Indications protection reform, to name a few. These laws include domain name registries in scope and put forward a set of obligations that influence the domain name registration process and domain name lifecycle.

As a result, operating a domain name registry in Europe or providing domain name services to European internet users is growing more complex and intensely regulated, bringing more compliance efforts.

4 How does CENTR's policy work help tackle issues related to DNS abuse?

CENTR members regard keeping abuse low on the internet as necessary in safeguarding internet user trust and safety within their zones. European ccTLDs are the zones with the minor level of abuse globally. The diversity of approaches towards keeping domain name zones safe and secure across European ccTLDs has multiple advantages, as it avoids the single point of failure for malicious actors to exploit.

At the same time, there is a general tendency to equate DNS abuse with cybercrime, as technically, all services on the internet rely on DNS. However, not all cybercrime can be mitigated and addressed at the DNS level.

Consequently, there is a need for a collaborative approach between multiple technical actors within the DNS ecosystem like registries, registrars, internet service providers, hosting service providers, etc, competent authorities, including law enforcement, and cybersecurity experts, such as CSIRTs to tackle different abuses online.

At CENTR, we encourage our members to exchange information and good practices with each other, informing the community about different approaches available for addressing abuse online within the technical limits of a registry.

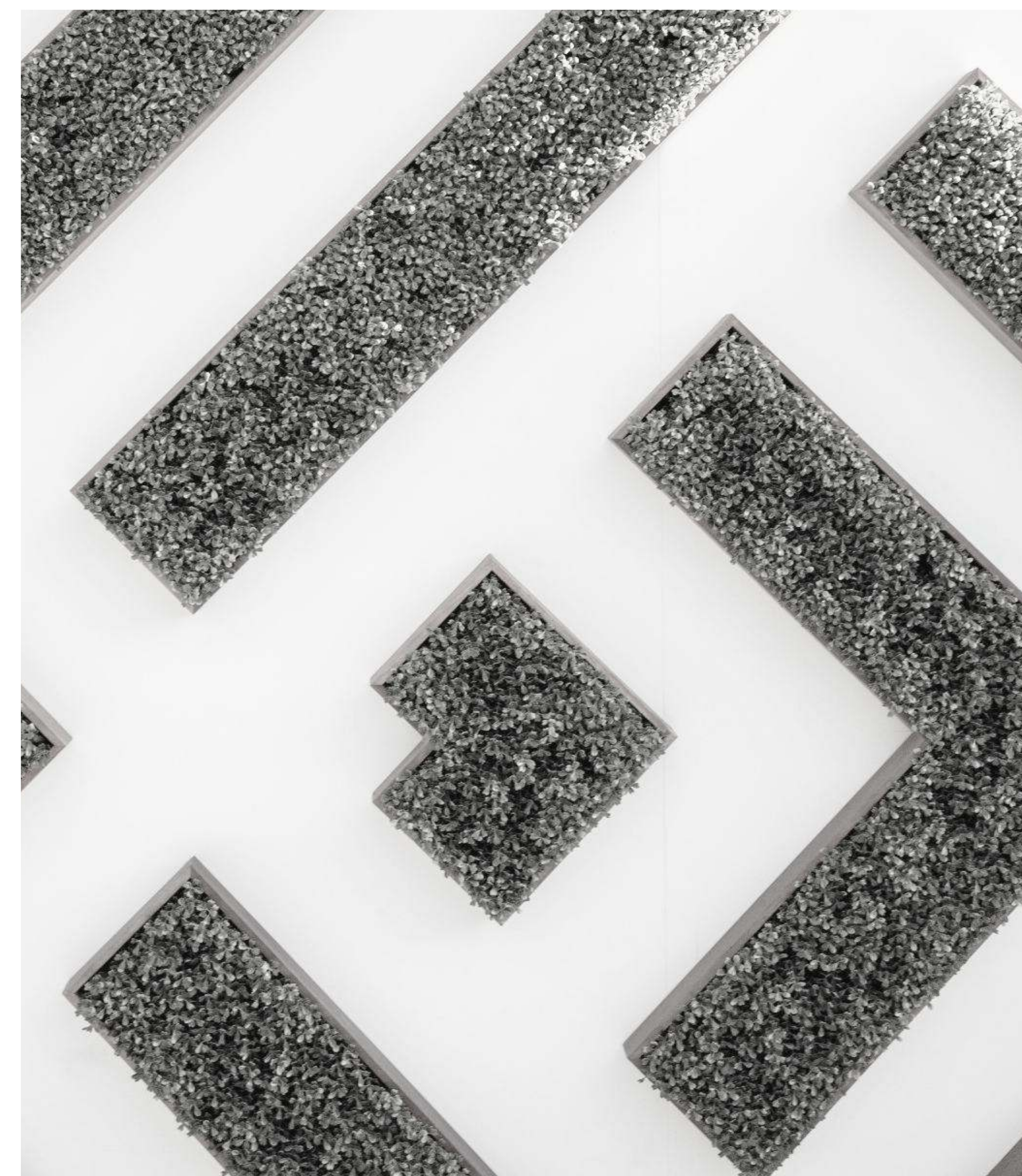
It is essential to remind policymakers that DNS-level action is not a silver bullet to end all cybercrime online and that DNS abuse is a misleading term.



Any action towards an abuse online mandated by a technical operator, such as a domain name registry, should be evaluated from the perspective of what is technically possible, proportionate with the level of harm, and most importantly, whether the harm can be mitigated and addressed by an intermediary that is closest to the source of abuse and without a drastic intervention at the infrastructure level.

5 With the NIS2 Directive on the horizon and member states soon to release their measures, what challenges do you foresee for ccTLD registries as they navigate this new landscape?

The NIS2 Directive introduces a set of obligations for ccTLD registries, as they are considered essential entities and vitally important for the functioning of society.



The NIS2 Directive aims to provide a minimum set of measures for cybersecurity preparedness of critical sectors, including TLD registries.

In addition, the NIS2 Directive introduced domain name registration data accuracy as one of the critical measures to maintain the DNS's stability, security and resilience.

These accuracy measures include an obligation on domain registries and registrars to verify domain name registration data, including the identity of a domain name holder. This verification obligation is one of the most challenging aspects of the NIS2 Directive for the domain industry, as it is unclear how far it is expected to go and which verification tools and measures would be acceptable for compliance with this obligation across the EU. There is also no uniform adoption of electronic identity across the EU that would facilitate verification of domain name holders, especially in a borderless and cross-border domain name market.

Finding the right balance between complying with accuracy obligations under the NIS2 Directive and maintaining a high level of cybersecurity of all registry operations while staying ahead of the curve of malicious actors who will undoubtedly explore new ways to circumvent identity checks is one of the biggest challenges with the expectations set by the NIS2 Directive. In addition, it is also important for Member States to keep the flexibility for ccTLD registries in addressing accuracy obligations, as the zone sizes, risk scenarios and registration processes are unique to each ccTLD.



Polina Malaja is one of the expert voices in our e-paper "Unraveling the NIS2 Directive". Gain insight into challenges and optimal navigation strategies.

There is no evidence to suggest that various approaches to registration data accuracy are detrimental to security. On the contrary, European ccTLDs are consistently referred to as the most secure domain zones at a global level despite having no unified approach to accuracy.

6 Data privacy is a hot topic these days. How do you foresee the relationship between data privacy policies and internet governance evolving in Europe?

Privacy and data protection have recently received much attention at the global internet governance level, primarily within the ICANN discussions. In Europe, however, European ccTLDs have balanced the need to protect domain name holders' data and law enforcement access to non-public domain name registration data for decades. To our understanding, there is no inherent conflict between privacy and security. The challenge for Europeans is to ensure that a high level of data protection in Europe is maintained as we go forward and not weakened by voices claiming otherwise. Data confidentiality is also part of the cybersecurity toolbox.

7 Are there any emerging trends in digital policy that our registrants and domain experts should be aware of?

In the last ten years, we have seen unprecedented regulatory attention to DNS and domain name registries, from cybersecurity to data and consumer protection, agriculture and financial policy in Europe. We expect this attention from EU policymakers to stay strong as DNS becomes increasingly ingrained in legislative proposals across policy areas beyond the usual digital regulation. This adds complexity not only in keeping up with these developments but also identifies the move towards interventions at the infrastructure level becoming more and more acceptable as an enforcement measure for a myriad of societal problems.

The challenge with these developments is to shed light on the broader repercussions of DNS becoming the vector for enforcement online, both for DNS operators and internet users. These repercussions often need to be included in impact assessments accompanying legislative proposals, which is a concern.

18 critical sectors

which are subject to the regulations set forth by the NIS2 Directive.

EU member states

that are required to implement the NIS2 Directive into their national legislation.

73 pages of the Directive.

72 hours

within which organizations must report an initial assessment of the significant incident, including its severity and impact.

46 articles

in the NIS2 Directive.

24 hours

hours within which organizations share an early warning indicating whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact.

[Read the full interview](#) →



Kelly Hardy

iQ, SVP Strategy and Development*

*Kelly transitioned to a different organization.

► The domain industry has a long development history and is a complex and multi-faceted sector, filled with diverse roles, responsibilities and nuances. It is an industry that demands versatility, adaptability and a broad set of skills. Navigating seamlessly across its varied sectors is no ordinary feat. One professional has consistently demonstrated exactly this ability, shifting between numerous positions in her career and showcasing her remarkable eclectic aptitude. Meet Kelly Hardy.

During her remarkable journey in the domain industry and internet infrastructure, Kelly has built a formidable career. With her expertise in international business development, channel management, policy and marketing/PR strategy, Kelly Hardy has left an imprint in the domain industry. She has woven success stories for a robust roster of well-known organizations, including Domain.ME, Afiliias, Blacknight and NamesCon, thereby forging a stellar reputation. Alongside her consulting work, Kelly has been a recurring figure on conference stages, moderating discussions, delivering powerful speeches and spreading her profound knowledge to transform and elevate businesses within the internet ecosystem.

IT'S ALL ABOUT BEING FUTURE-FORWARD YET USER-CENTRIC!

Decipher the codes of the domain industry as this domain visionary shares her insider insights. Buckle up for a captivating conversation.



Join us in this talk with Kelly Hardy as she exemplifies the power of adaptability and diverse expertise in the multifaceted domain industry!

① *How did your personal and professional experiences shape your path toward the domain industry?*

I originally come from the music industry. I've co-owned a magazine and a small record label and spent some time working for record companies.

In the early 2000s, I was involved with a firm specializing in brand protection and started working with the ICANN community, a step that would pivot my professional life in an exciting new direction. My interest in the domain industry grew unexpectedly and as my work thrived, I delved deeper into this captivating field.

After working a couple of years within the industry, I laid the foundation for my own consulting firm in 2009. It has proven to be a marvelous adventure so far. My clientele is a roster of who's who in the industry and I've had the privilege of working with renowned entities such as .ME, CoCCA, CentralNic and, most recently, iQ as a SVP Strategy and Development.

② *As an experienced domain professional, you must have seen many transformations in the industry. What evolution in terms of trends and changes have you seen over the years?*

As an experienced domain professional, you must have seen many transformations in the industry. What evolution in terms of trends and changes have you seen over the years?

The transformation within the domain name industry was substantial after introducing the new gTLDs. What had been a very static, close-knit niche community was suddenly inundated with fresh perspectives and a diverse array of individuals.

There are some things about the pre-new gTLD industry that I miss a lot. Earlier, the domain industry was less complex, making navigating the available options easier. Stakeholders felt a sense of familiarity with the limited domain offerings, leading to more straightforward decision-making.

But things needed to evolve to foster a diverse and inclusive environment. Demographics needed to change. Nowadays, it is a more diverse industry than it was ten years ago. It was essential to break the homogeneity of the industry demographics and embrace stakeholders from various backgrounds, ethnicities and genders, which has since been achieved to an extent.

As good stewards of the internet, our responsibility extends beyond maintaining the status quo. Change is important. As a global platform, the internet continuously witnesses a broad range of alterations like technological upgrades and evolving legal landscapes, like GDPR and the NIS2 Directive.



3 *The domain name industry, similar to other sectors, is subject to a dynamic policy environment. How do you navigate policy changes?*

I've been engaged in policy assistance and consultation for nearly two decades. This vast experience has influenced my professional role in adapting to the shifting regulatory landscape.

My job mainly entailed interpreting legislation and related information provided by ICANN. Also, it included the critical task of developing policy and crafting necessary agreements based on these guidelines.

However, my job responsibilities have substantially evolved with the increasingly interconnected and complex global economy. Nowadays, I am more involved in guiding our clients in preparing and adapting their business operations to comply with new international regulations and legislations. Recently, one of the key focal areas of my work has been tackling the issue of DNS abuse. Understanding and mitigating DNS abuse has become crucial in this rampant cyberattack era. Taking conclusive actions against such violations signifies regulatory compliance and is considered a best practice.

My experience and striving to prevail against ever-evolving challenges have enabled me to effectively assist, advise, and guide organizations through their legal and technical endeavors. This way, I help them navigate their policy-related concerns, preparing them to face an ever-changing digital landscape head-on.

4 *In recent years, the domain industry has experienced a surge in growth and innovation driven by various emerging technologies. What role does technological advancement play?*

In recent years, the domain industry has experienced a surge in growth and innovation driven by various emerging technologies. What role does technological advancement play?

By its nature, the domain industry can often exhibit skepticism toward accepting or incorporating new technologies. While this reservation might seem prudent to maintain stability and tried-and-true processes, it could impede productivity growth and innovation. Therefore, our sector must adapt and integrate new, promising technology to stay relevant, innovative, and prepared.

My work at iQ nowadays involves cybersecurity services and business intelligence insights. In line with consistently delivering secure and smart solutions, our team has been leveraging recent advancements in AI to bolster our capabilities. Our primary focus has been enhancing detection and mitigation methodologies related to domain abuse and various online harms.

Failure to do so might lead us to a future where we could find ourselves ill-prepared against evolving threats or challenges in cyberspace that could have been warded off if only we had welcomed and harnessed the potential of emergent technology earlier in the timeline.

The domain industry should focus on combating abuse at all levels: server, content and domain. To achieve this, it's vital to understand the need for employees to think outside the box and embrace team play. These factors contribute to a more practical approach to tackling abuse, impacting the industry positively.



5 *What is a particularly challenging project you've worked on and how did you handle it?*

A few years back, we faced a complex, high-profile content abuse takedown project. Thinking outside the box and adapting to challenges was essential to finding practical solutions. As it's not our area of expertise, our industry often avoids making content-related decisions. However, sometimes, a TLD hosts harmful content, making intervention necessary.

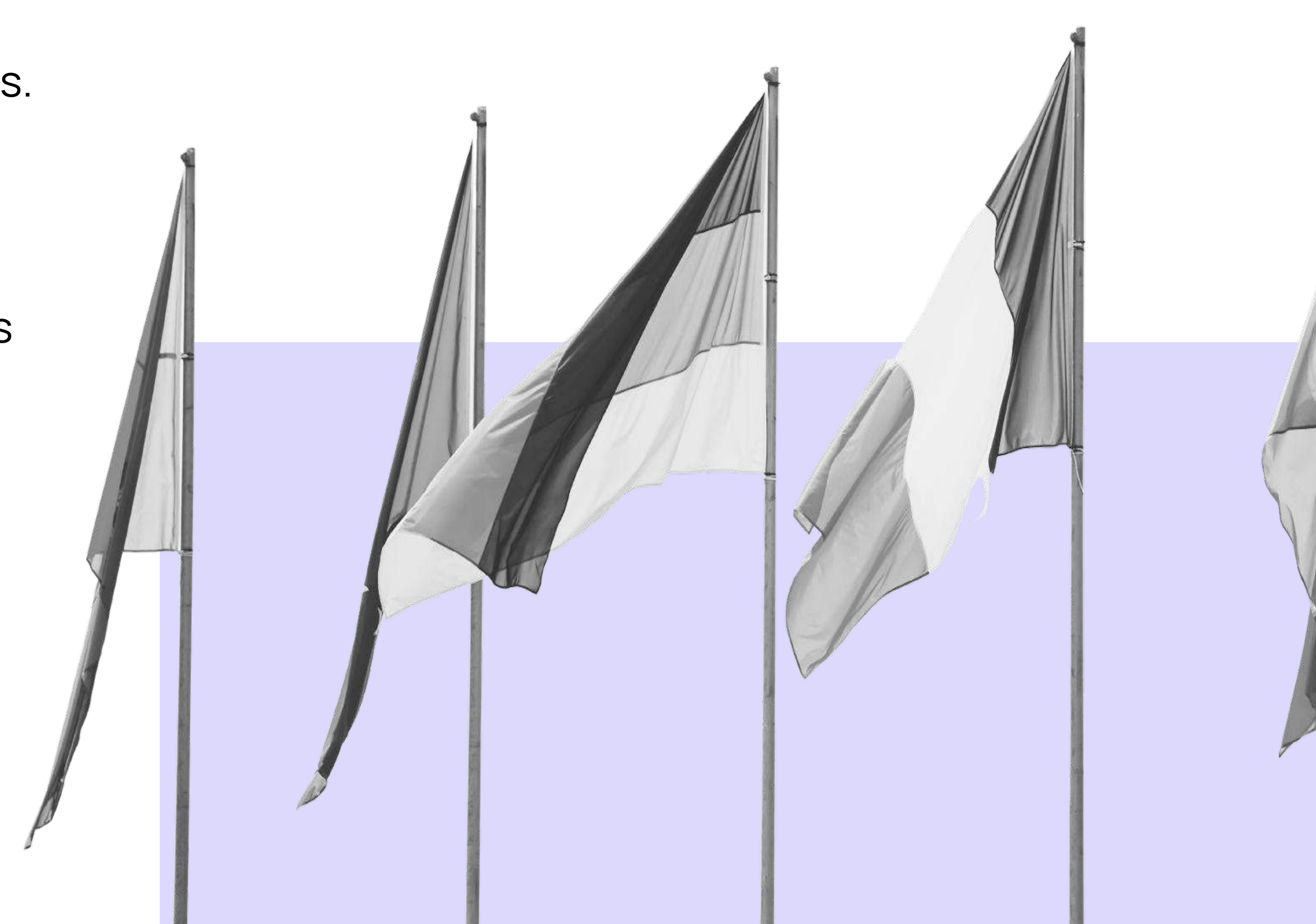
This demanding project, beginning as a moral debate over terms of use violation, eventually became a more significant issue than initially expected, spanning several months. Luckily, I had the support of an exceptional team that demonstrated the importance of teamwork and collaboration in such complex situations.

The domain industry should focus on combating abuse at all levels: server, content and domain. To achieve this, it's



vital to understand the need for employees to think outside the box and embrace team play. These factors contribute to a more practical approach to tackling abuse, impacting the industry positively.

It cannot be overstated how crucial it is for companies to combat abuse actively. This approach benefits both their reputation and their employees' morale. By fighting abuse, businesses showcase their commitment to ethical practices, attracting customers and gaining employee loyalty. These measures help shape a secure, inclusive environment that enhances productivity and job satisfaction.



7 *What are the key competencies and technical skills to succeed as a registrar or TLD registry?*

I could talk about this all day, but here are four essential components to keep it short.

→ **Flexibility:** The domain world is constantly changing. Hence, it is integral to remain adaptable in response to these fluctuations. Sometimes, your TLD's perceived use or target audience differs from what your customer base seeks. Being flexible and open-minded towards these changes can pave the way for better business success.

→ **Effective communication:** As a registrar or TLD registry, you are a custodian of the internet's infrastructure. It's crucial to communicate this value to your customers effectively. In essence, you are "selling air" – domain names, hosting and security are intangible yet vital parts of the internet. If you can't articulate the significance of these services to your customers or spark their interest in them, it could become a stumbling block in your path to success.

→ **Market awareness:** Knowledge about the market you're serving and customer needs is vital to running a successful business. A keen market awareness helps you understand your customers' changing needs and adapt your business strategy accordingly.

→ **Customer-oriented thinking:** Lastly, keeping your customers at the forefront of your decision-making process is crucial. This involves listening carefully to your customer's needs, even if they differ from your initial business plan. Successfully meeting their demands and riding the wave of changes will lead to a more successful and credible registrar or TLD registry business.

8 *How might the domain industry's future adapt to the digital landscape's progression and new trends?*

The future of the domain industry lies in fostering continual innovation and safeguarding its critical infrastructure. It necessitates embracing new technologies like AI for domain management and maintaining a secure, accessible internet environment. Shaping the industry's future involves understanding users' ever-changing needs and technological trends, ensuring its relevance and value. As the digital landscape evolves with developments like 5G and IoT, the domain industry must adapt accordingly, guaranteeing a safe, privacy-respecting online space for current and future users. It's all about being future-forward yet user-centric!

[Read the full interview](#) →



Ron Jackson

DNJournal.com, Editor & Publisher

► One market in the domain industry has shown remarkable growth and dynamism: domain investing. As this sector expands, the need for reliable, up-to-date information becomes paramount.

Enter [DNJournal](#), a beacon of knowledge and insight for those navigating the intricacies of domain sales and developments. Founded on 1 January 2003 by Ron Jackson, a seasoned editor with a keen eye for the domain industry's pulse, DNJournal has become an indispensable resource. With its comprehensive coverage of domain name sales across all registries and geographies and a commitment to publishing year-to-date sales data, DNJournal is undeniably a cornerstone of our industry.

Ron Jackson, DNJournal's Chief Editor and President, brings his expertise and collaborative spirit to the forefront of the domain investing community. His professionalism and dedication have made DNJournal a publication and a platform where industry trends are reported and analyzed.

Join us as we delve into an exclusive interview with Ron Jackson. Get to know the man behind DNJournal, explore the roots of his editorial project and gain professional insights into domain investing.

IF YOU CAN'T BEAT THEM, JOIN THEM!

A conversation through the vibrant world of domain investment with insider knowledge and expert insight.



This is your opportunity to peer behind the curtain of the domain market's leading publication!

❶ *What led to the creation of DNJournal? What gap in the domain investing market were you aiming to bridge?*

When I first discovered the domain industry in 2002, I had no plans to start a publication.

After 20 years in broadcasting and journalism (print, TV and radio), I decided I wanted to work for myself, so I returned to my other first love, music and opened a chain of record stores.

One of the three music stores run by Ron Jackson before he entered the domain industry and launched DNJournal. I had a great run in that business for the next 12 years, but then the internet came along, and the ability to download music, coupled with the arrival of CD burners that allowed unlimited copying,

wiped out almost every record store in the US, including mine. In 2002, I suddenly had to find a new line of work.

The only thing I knew about domains was that I registered one in 1997, which I used to create a website for my music store: musicparadise.com. Having been wiped out by the internet, I decided that anything I did in the future would have to focus on the web because it was disrupting one industry after another. It was a classic case of "if you can't beat them, join them!"

I knew I would need a new domain name for whatever I did, so after thinking about what kind of work I might want, I started looking for a few domain names that would match those ideas. While doing that, I stumbled upon DNForum.com, where the members talked about buying and selling domain names alone.



One of the three music stores run by Ron Jackson before he entered the domain industry and launched DNJournal.

2 *What examples of successful domain name investments have you made or seen in the industry?*

The investments that attract people's attention are the high-end sales, six and seven-figure transactions involving domains that the original owner may have picked up for under \$100.

Some got their domains for free, like my friends Michael Castello and his brother David from Castello Cities Internet Network. Michael registered many great names in the mid-1990s, and they have given him eye-popping sales like whiskey.com at \$3.1 million. Many of Michael's contemporaries have done the same thing with legendary results and most of their names are known far and wide now: Frank Schilling, Rick Schwartz, Kevin Ham, Scott Day, Garry Chernoff, Nat Cohen and many more whose names would fill this entire page if I kept rattling them off.

Having concentrated on the small business market, it has been more about building a revenue stream with many affordable domains that consistently sell. I have a portfolio of about 2,000 domains and my turnover rate in recent years has been 3-4% annually. People commonly think that the average turnover rate for a portfolio is 1-2%. At this point, I can renew almost the entire portfolio every year and it will spin off a decent revenue stream year after year from sales alone.

3 *As a veteran in the domain name industry, what trends have you observed since you began investing in 2002?*

It has been wonderful to see the industry grow into what it has become today and see much more of the mainstream business world finally understanding the value of the right domain to their enterprise. There is still much room to grow because many businesses still don't understand that, even though the COVID-19 pandemic certainly woke up thousands of them worldwide. That was when so many suddenly realized they would be out of business if they didn't build or improve their online presence immediately.

The primary constant force in the industry has been consolidation, with the bigger, well-capitalized companies swallowing up innovative smaller ones—but that has always been the way of the business world and is not surprising.

4 *What common mistakes have you observed in the domain investing market? How can investors avoid them?*

The big mistake I and almost every new investor made was diving in head first and hitting my head on the bottom of an empty pool. For most of the people who came in when I did, the second wave after the original pioneers, we were mostly flying by the seat of our pants and following gut instinct. That's because I didn't take the time to learn what makes a given domain valuable and, more importantly, how valuable a particular name is so you don't overpay for it and will have a decent chance to profit.

You learned by trial and error – which is effective but can also be very expensive! We would buy a lot of stuff and see what would sell and what wouldn't.

There weren't many places to learn from. Blogs did not even exist then. DNJournal tried to help with our regular domain sales reports that give readers a long list of recent sales showing them the exact price paid for specific domains so they could learn from studying those examples before spending their money. It used to take a year or two to start getting a handle on what worked and what didn't. Today, there are many more resources to draw on like your Snapshot, including complete educational programs.



"In the domain business's early days, we had mostly not met in person, each working from home behind our computers. This changed in October 2004 with the first major domain conference, TRAFFIC, in Delray Beach, Florida. At the second TRAFFIC show in October 2005, also in Delray Beach, co-founder Rick Schwartz (the Domain King) honored me with a special "Public Awareness of Domains" Award. This award recognized DNJournal's pioneering coverage of the industry, highlighting the existence and value of domains as assets."





5 *You own a significant number of three-letter "us" domain names. What motivated you to invest in this ccTLD?*

I have an affinity for .us because I discovered the domain business thanks to it. It was back in the spring of 2002 when I was trying to figure out what I would do for a living after closing the record stores. I was building my computers, so I subscribed to many computer magazines.

A new issue arrived one day and inside the front cover was a full-page ad placed by the .us registry announcing that the TLD would be opened to all US citizens on 24 April of that year. In the 17 years before that, .us, the first ccTLD on the internet created on 15 February 1985, was available only to a limited pool of users like government, schools and law enforcement.

I remember that when I went looking for my record store domain in 1997, the actual name of the store, Rock Island, had already been taken to .com.

I settled for MusicParadise.com and eventually changed the store's name to match.

I saw the .us ad and thought this was an excellent opportunity to get some high-quality keyword domains for the ideas I had in mind. It was before I discovered the business of buying and selling names, but the ad started me on the journey that led me to the business.

I also like the dual function of "us" in a domain name. In addition to being a ccTLD of the United States of America,

the word "us" gives organizations more options for creating catchy domains.

Looking at the American small business market, I knew many couldn't afford a short .com or the one they needed might not be available at any cost. I thought they might be attracted to this new .us alternative. I gathered hundreds of them in those early years and they have paid for themselves every year, though they have only started paying off at a significantly higher level in recent years. I credit the ubiquity of zoom.us for spreading .us recognition, along with the explosion in the number of new gTLDs that has created awareness that there are now a lot of options on the other side of the dot.

6 *What does the future hold for the domain name industry?*

From day one, 22 years ago, I have always been optimistic about the future of domain names, and that has never changed, especially not now when I see that the mainstream business world still needs to fully grasp how important the right domain is to its enterprise.

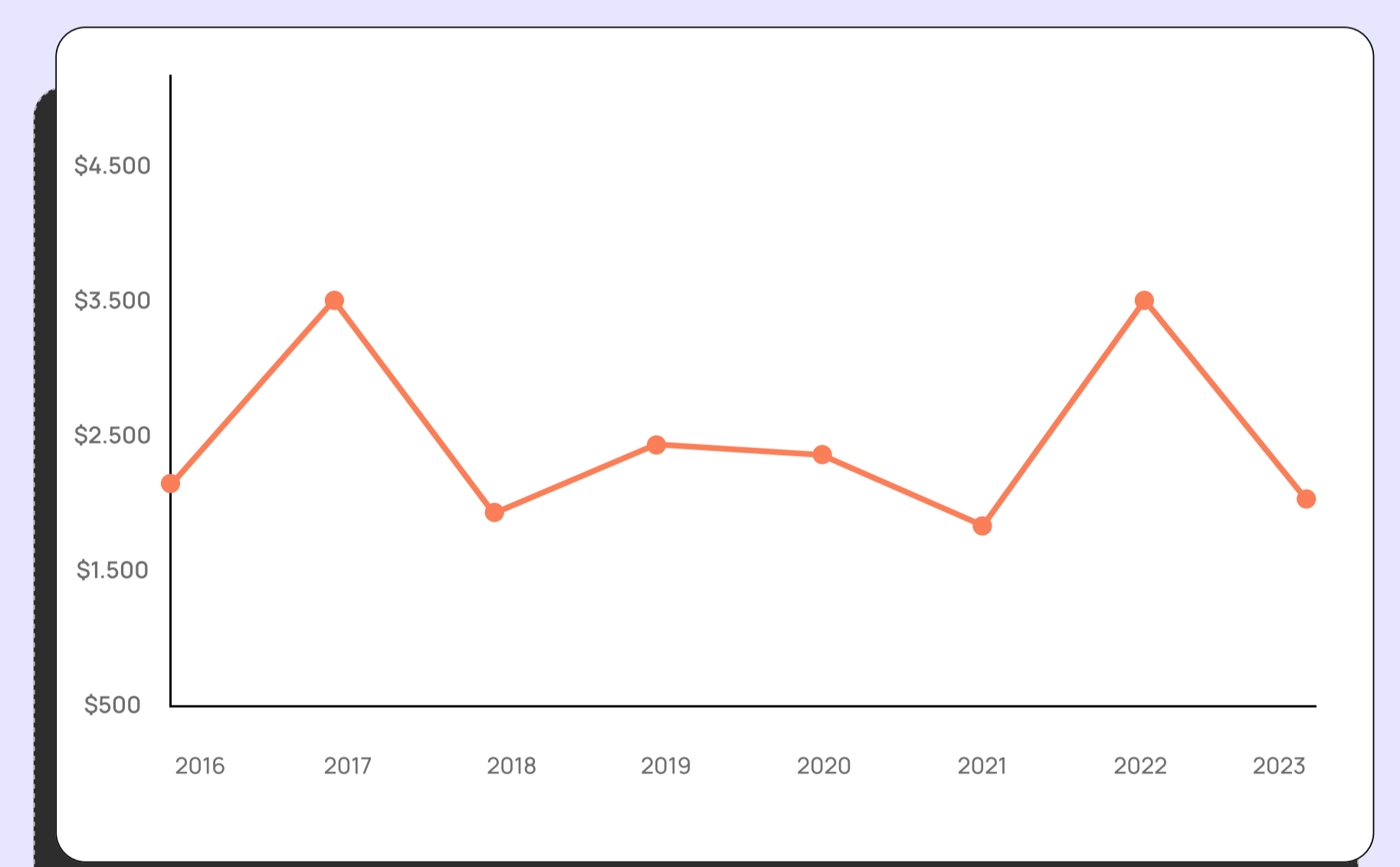
We have made enormous strides in that regard and many people have done very well in this business because of it. I still see room for growth and new converts.

Even if you don't buy, sell or trade online, the web is where people go to find out where you are, more about your product and services and how to contact you. I know many people use social media instead of their site, but that is not much better and can be highly hazardous to your financial health.

You are putting your business at the mercy of some corporation that can quickly put you out of business for violating some arcane rule – and they won't even tell you why they shut you down! Be smart – get your domain name and build your own website.

As for DNJournal's place in it, I expect to see the status quo maintained, and I am happy with that as I love everything I do. Thanks to our advertisers, we have always received the resources needed to cover the industry and the many extraordinarily creative people who make it a wonderful field.

Median price of sold .ai domains



Since I expect the industry to continue doing well in the years ahead, I feel very good about the prospects not only for DNJournal but for every domain professional who is reading this – and I wish the best for all of you!

[Read the full interview →](#)



Radix, VP Channel Partnerships

► The relationship between domain registries and registrars is the backbone of the internet's naming system. Forging solid relationships and collaborations is crucial to success in this interconnected ecosystem. These entities collaborate to manage vital components of the DNS, ensuring that domain names are accessible and secure.

Neha Naik, VP of Channel Partnerships at Radix, is responsible for nurturing these vital connections in the domain industry. With her 17-year tenure mapping across various industry giants, Neha's expertise is not just in forming alliances but strengthening the fabric of the domain industry's network. Neha has been pivotal in enhancing Radix's partner network and fostering enduring business relationships.

As we delve into this fascinating conversation with Neha, expect to uncover rich insights on how robust industry relationships drive the technical and business strategies of a major registry like Radix!

OUR GOAL IS TO FIND ALIGNMENT SO WE CAN GROW TOGETHER!

Cultivating and maintaining critical industry relationships shapes the future trajectory of domain registries and registrars.



1 What is your career journey in the domain industry and how did you get involved with Radix?

The world of domains came calling in 2005. I started as a fresh recruit, out of college after having completed my degree in Mass Media and I took up a role with the parent company of Radix, which was Directi back then.

Little did I know I was foraying into a fascinating and omnipresent industry. It impacts almost everything we do online. DNS and domains: Words that not everyone knows but really ought to! After a few businesses and a few different roles, we decided to explore the registry business and that's when Radix was born in 2013 - I'm proud to have been part of this journey since then!

2 As a key player at Radix, what does your role entail daily?

My role focuses on the Channel Partnerships side of the business - building, growing and innovating what we do with our partners. Our Channel Partners: registrars, hosting companies, resellers and the entire gamut of domain providers are core to our business. Our goal is to find alignment so we can grow together!

Every day is different. While Radix has been around for over ten years and has grown to almost 10 million domains, we are still very rooted in our desire to be radically different.

Fun fact: The word radical comes from the Latin word Radix, which means the "root"; something that changes, addresses or affects the major essence of something. We're often referred to as the Radix Radicals and our persistent desire to innovate and do things differently remains at the heart of our operations. That makes life at Radix very interesting!

We're lucky to be in an industry that allows for personal connection through meetings and conferences throughout the year. We have been fortunate to build lasting relationships with many amazing people. At the core, partnerships are building relationships with people we work with and that is the part of my role that I love the most! Finding genuine connections with people you work with!

3 Radix has risen to become the largest new gTLD registry worldwide. What has been the company's strategy behind this success?

Radix has always focused on high-quality, broad/generic TLDs with a wide addressable market that resonates with users across verticals. You can see that in the TLDs we manage .online, .store, .store, .site, .tech to name a few. To take that even further, we have a superb team



of creative, highly motivated folks who want to see Radix succeed beyond what's obvious!

In addition to our strong TLDs, Radix has focused on building awareness of them. Each TLD is treated like an individual brand with its own target audience and its own brand essence. Our Brand Managers have been creating TLD awareness in their respective segments. For example, .store with the ecommerce community, .tech with startup founders and .online among SMBs.

TLDs that resonate widely with the target audience, characterized by high awareness and desirability, will become the more apparent choices for consumers. Awareness building begins with us as a registry and then continues through our channel partners.

We've also made significant strides in understanding the needs, challenges, goals, and behavior of the actual end users of our domains. Our goal is to create something of value for these users by truly understanding what can help them do more and better!

I credit Radix's success to the specific TLDs we manage, of course, but more importantly to the team and the vision of what we have set out as our goal in the years to come.

4 What challenges do you face in managing such a vast portfolio of gTLDs?

We have a portfolio of 11 gTLDs and while we have TLDs focused on specific verticals like .store for ecommerce or .tech for startups, we also have our generic TLDs like .online, .site and .website. One of the biggest challenges we faced earlier was the focus. How do you focus on so many TLDs at the same time? This is why we decided to bring in Brand Managers within our marketing teams, each responsible for a TLD and focused on growing their specific audiences, finding their niches and scaling from there on. Another challenge common to most registries is that you are not directly connected with the end customer. You are one level separated because they register their domains from a registrar like InterNetX or their domain resellers and not from the registry. This separation makes it harder to understand the customer base and their needs. This understanding is critical to building a sustainable business and you have to launch initiatives to gain an end-user perspective.

RADIX PREMIUMS GROWTH YOY



There are several upsides to a portfolio registry, though – for starters, you have economies of scale. You get to learn quickly from experiments run by one TLD and apply it to another. Your learnings and your experience are actually manifold. You have so much more data to make decisions and move quickly. You also have the opportunity to build much broader partnerships that could address different audiences of the domain industry.

5 With e-commerce booming, how have TLDs like .store been positioned to benefit online retailers and customers?

We have seen the percentage of ecommerce websites grow to 28%+ of all developed websites. This is a clear sign that e-commerce adoption is steadily increasing. Moreover, we have seen 3x growth in live websites on .store since January 2021, portraying strong adoption of the .store TLD for online businesses. And there is nothing better than a .store that sends a clear signal that you're a website looking to sell something!

We've also seen very good traction on ecommerce platforms like Shopify. The TLD .store is the second highest-selling TLD on their platform after .com!

Adoption from several celebrities and Youtubers has also validated the acceptance and need for the TLD. I could mention the singer Shakira using shakira.store or the band Maroon 5 using maroon5.store for their respective merch stores.

We had an independent agency conduct an SEO-focused study. The study found that businesses using a .store domain benefit from double the visibility

compared to other domains and enjoy a 12% higher Return on Advertising Spend (ROAS). Choosing a .store domain could significantly boost your sales! There are distinct benefits for calling out what your online presence is for and .store accentuates that very well!

6 What trends have you observed in TLD profitability and how does Radix prioritize investment in different domains?

The premium domains model we follow is a high-high model, which means these high-value, high-quality names register and renew at premium pricing, ranging from \$100s to \$1000s annually.

According to Radix Premiums report 2023, we've grown over 25%+ YoY with over \$4.8M in premium sales in H2 2023. These registrations see a stellar renewal rate of 57% on the first time and 80%+ on the subsequent years. It truly showcases the model's success and the value these names provide users.

Some of our premium name success stories include the likes of online food delivery giant Doordash using order.online, self-driving technology company Aurora, using aurora.tech, having raised \$4.2B in funding to date and several more.

[Read the full interview →](#)



Elias Rendón Bengler

InterNetX, CEO

► In a world where domains have become the cornerstone of digital identity for brands across the globe, it's forward-thinking skills and leadership that redefine boundaries and ensure that businesses thrive in the evolving tapestry of the internet. Elias Rendón Bengler is a prime example of such leadership, steering InterNetX towards new horizons of success and influence within the domain industry.

Elias's academic background in business administration set a strong foundation for his impressive career path, one that has taken him across the globe as he delivered IT consultancy services to large enterprises in the financial services, automotive and telecommunications sectors. His aptitude for leadership was clear, as evidenced by numerous roles in product management at IONOS, where he honed his skills in global marketing and commercial management.

At InterNetX, he has placed a strong emphasis on domains as a tool for growth and internationalization, recognizing their intrinsic value and potential to empower businesses worldwide. Appointed CEO in 2023, Elias Rendón Bengler now brings that same commitment and strategic insight to a broader stage, advocating for being the innovation pacemaker and trusted advisor in the domain industry and being the domain business leader for the whole IONOS Group.

Join Elias Rendón Bengler in this interview, as he shares his valuable perspective on the future of domains and how InterNetX continues to shape the digital landscape for businesses around the globe.

IT'S IMPORTANT TO VIEW CHANGES AS CATALYSTS.

Each hurdle has pushed us to adapt and innovate to overcome these turbulent times.



❶ *Since assuming the leadership at InterNetX, what are the core guiding principles and strategic advancements you're implementing to propel the company into its next era of growth in the domain industry?*

As the CEO of InterNetX today, I am honored to steer a domain industry pioneer into its next chapter.

The vision I share with my colleagues is to make InterNetX a pivotal domain hub, connecting our business partners under the IONOS roof on one side and our clients on the other. We're on a mission to redefine the way businesses interact with domain services to stand as the leader in end-to-end domain solutions. At the same time, we're cementing our position as the backbone of the IONOS Group's domain expertise, ensuring that our integrated management solutions are the benchmark in the industry.

At InterNetX, we see domains as vital assets. We've got a deep understanding of the market and the specific needs of enterprises, resellers and domain investors.



We're equipped with top-notch IT skills and the knowledge necessary to develop tailored solutions and offer unparalleled services. By leveraging our extensive TLD portfolio and innovative tools like AutoDNS, we aim to set new benchmarks in domain services. For example, we recently integrated direct access to the

Sedo aftermarket into AutoDNS. This means users can now easily buy, sell, manage and monetize domains in one single platform.

InterNetX is dedicated to being the global domain specialist, offering more than just domain registration—our holistic approach includes hosting, security and tailored brand protection solutions, ensuring our partners excel through reliability, performance and true expert support in this digital age.

❷ *Diving into the complexities of the domain industry, what have been some of the most significant challenges and how have you addressed them?*

I stepped into my role as InterNetX CEO aware of the global headwinds reshaping our sector and the economy. Each hurdle has pushed us to adapt and innovate to overcome these turbulent times.

In response to the challenges posed by recent global events, including war, geopolitical tensions, the energy crisis, and rising inflation, we've faced increased operational pressures. To navigate these hurdles, we've taken strategic steps. We've honed our resource management and enhanced our commitment to digital trust by focusing on even more secure digital services. This ensures that your data stays safe and your digital experiences remain smooth and uninterrupted, despite these challenges.

Transitioning to new working models post-pandemic holds challenges and opportunities alike. We embraced flexible working models, harnessing advanced collaborative technologies and flexible schedules to maintain productivity and employee satisfaction.

And then there's the big game-changer: artificial intelligence (AI). This technology is transforming the domain industry,

from predictive analytics in domain valuation to AI-driven security measures. At InterNetX, we recognize AI's decisive role as a disruptive trend and are making it part of our DNA, compelling us to place it at the forefront of our discussions and explorations, like in our Global Domain Report 2024.

All of this in the framework of general market consolidation, crucial for enterprises, challenging SMEs to either scale or get left behind by the bigs of innovation and versatility. It's a pivotal moment that calls for both a strategic rethink and a bold leap for those looking to thrive amidst these giants.

As the landscape changes, so do we. It's important to view changes as catalysts for innovation and growth. This vision propels us forward, setting the tone for the domain industry's future and for us as a business.

3 *From your perspective, how has the domain industry evolved over the recent years and where do you see it heading?*

It's been a whirlwind of evolution and innovation. The domain industry has transitioned from its early, volatile 'Wild West' phase into a structured and mature market, forming the backbone of billion-dollar enterprises and innovative digital unicorns that are now "flirting" with blockchain technologies. It's fascinating to see just how much has changed—and where we're heading next.

The new gTLDs have been nothing short of a revolution, with new ones added to our [TLD portfolio](#) every year since 2016 and a whole new wave set to break with the 2026 new gTLD round.

For those of us in the domain service business, this translates to a blend of partnership with registries and technical effort to ensure seamless integration for our users. With the onset of COVID-19, the spotlight on security and brand protection intensified.

As businesses rushed online, the digital space became crowded, turning domain security and protection against DNS abuse into top priorities. The pandemic taught us the critical importance of safeguarding our digital identities against a backdrop of rising cyber threats. This focus on security is a paradigm shift, ensuring businesses and individuals alike are better protected. The domain aftermarket, too, has



witnessed remarkable growth. It's a vibrant marketplace, bustling with activity, where domains are bought and sold, often at premium prices. This aspect of the industry highlights the enduring value and demand for high-quality digital real estate—a trend that shows no signs of slowing down.

Amidst it all, regulations have tightened. The increased attention on privacy, data protection and cybersecurity with the NIS2 Directive having an impact on the domain industry has ushered in a wave of new policies. Compliance has become a key consideration for everyone in the domain space. These evolving regulations are a double-edged sword, bringing both challenges and a greater sense of accountability and trust in the digital world.

Looking ahead, it's clear that the fusion of innovation, security and technology will continue to drive the domain industry forward. For those of us active in this industry and working with domains, these are indeed exciting times.

4 *How is InterNetX gearing up for the NIS2 Directive, and what specific measures are being implemented in response?*

There will be sweeping changes in the domain industry because of the NIS2 Directive. We are proactively undertaking comprehensive compliance and legal reviews to align our operations with the new requirements. Our emphasis on enhancing risk management processes and data protection measures underscores our commitment to cybersecurity resilience. We've streamlined our incident reporting

protocols to respond to any breaches, ensuring transparency and effectiveness. Importantly, we're reinforcing collaboration with our TLD registries, sharing threat intelligence and best practices to bolster collective cyber defenses.

Our expertise in domain management equips us to navigate these challenges. SMEs and resellers that rely on InterNetX's DNS and domain services can have peace of mind knowing that compliance with the latest regulations is handled by us.

With our active leadership in industry discussions about the NIS2 Directive, we're at the forefront in ensuring that our clients can devote their attention wholly to their businesses, free from the complexities of regulatory adherence. We simplify compliance, managing all aspects on their behalf, so they can concentrate on what they do best—growing their venture in a secure digital space.

5 *With the anticipation of a new gTLD round, what opportunities and challenges do you foresee for InterNetX and the domain industry?*

The new gTLD round 2026 is a big shift in the history of the domain industry that comes with great opportunities and significant challenges. For businesses, it's a golden opportunity to target a particular niche and offer domain names that resonate with their brand and values. For instance, the introduction of .xyz was initially met with skepticism, yet it has defied expectations to become the leading new gTLD worldwide. This diversification of choice breathes new life into the market, pushing the boundaries

of creativity and innovation. Imagine a startup opting for a tech TLD like .tech to immediately convey its industry. Or an online shop choosing a .shop domain to increase its appeal. These examples showcase how businesses can leverage unique domain extensions to stand out in a crowded online space.

The new gTLD round 2026 is a big shift in the history of the domain industry that comes with great opportunities and significant challenges. For businesses, it's a golden opportunity!



However, a new set of new gTLDs heightens the competitive landscape. For businesses in the industry, staying ahead means providing the best value and service in a market that's more crowded than ever. There's also the issue of consumer confusion. With so many options, users may feel overwhelmed and unsure of which domain best suits their needs. Each new gTLD also opens another window for intellectual property concerns, demanding vigilance and strategic foresight to ensure brands are protected across all domains.

For a registrar like us, the technical implementation and administration of so many new gTLDs is no small feat. It's a complex mix of updating systems, ensuring compatibility and maintaining seamless user experiences across all touchpoints.

As a registrar with over 25 years of experience, InterNetX makes sure that new gTLDs are integrated as smoothly and securely as possible. It's a journey we embark upon with optimism and determination, since we are armed with the expertise and innovation that enables us to face this challenge.

6 *What advice would you give to aspiring entrepreneurs looking to make their mark as a domain reseller?*

For entrepreneurs starting up in the domain reselling business, the journey can be rewarding and present unique complexities.

To effectively navigate the domain industry—a field characterized by ever-evolving trends and shifts—it's imperative to chart the course with a keen eye and curiosity. Our [Global Domain Report 2024](#), together with our rich content hub [Snapshot](#), offers a solid foundation. It equips you with the foresight and expert tips needed to navigate the domain industry, giving you access to the latest data and know-how to maintain a competitive edge. Establishing your niche is another important factor. It's about precision targeting, finding the unique intersection where your expertise meets demand and (why not) your passion. This specificity is what will set you apart in a crowded marketplace.

Partnering with a reliable registrar can make the difference, allowing you to focus more on the selling rather than setting up and maintaining your business solutions.

Support is a cornerstone of our offering. Exceptional customer service ensures you're never navigating solo. Last but not least, networking is the final piece of the puzzle. Engage, connect and grow within the community. This year in Frankfurt, we proudly organized the Domain Summit, bringing together key players of the domain industry to foster networking and knowledge exchange, highlighting our instrumental role in connecting the domain community. Support is a cornerstone of our offering. Exceptional customer service ensures you're never navigating solo. Last but not least, networking is the final piece of the puzzle. Engage, connect and grow within the community. This year in Frankfurt, we proudly organized the Domain Summit, bringing together key players of the domain industry to foster networking and knowledge exchange, highlighting our instrumental role in connecting the domain community.

For those poised to make their mark as domain resellers, the path is laden with opportunities. Our Reseller Program is crafted to arm you with an arsenal of tools, ensuring your journey is not just successful but also scalable.

7 *How does InterNetX's expertise in building partnerships elevate businesses within the domain industry?*

Our role at InterNetX is rooted in fostering strong partnerships that elevate our position in the industry while also empowering the businesses we collaborate with. Leveraging our long-standing networking skills and an

expansive network, we've maintained relationships with hundreds of TLD registries and industry partners.

This network allows us to engage in widespread joint marketing activities. For example, we collaborate with TLD registries to exchange valuable content and position them as leading voices in our [Global Domain Report](#), amplifying their expertise and insights within the industry. The collaboration and support from Radix, Identity Digital, it.com, and Sectigo were instrumental in realizing the [Domain Summit 2024](#), an event that underpins our commitment to fostering connections and sharing knowledge within the domain industry.

A recent example of our innovative approach to partnerships is our collaboration with the American football team, Frankfurt Galaxy, supported by EURid. This partnership transcends the traditional boundaries of our industry, uniting the worlds of technology and sports, and showcases the expansive collaboration potential when diverse sectors align under a shared vision.

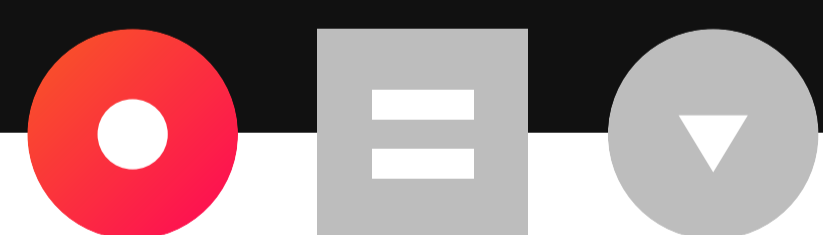
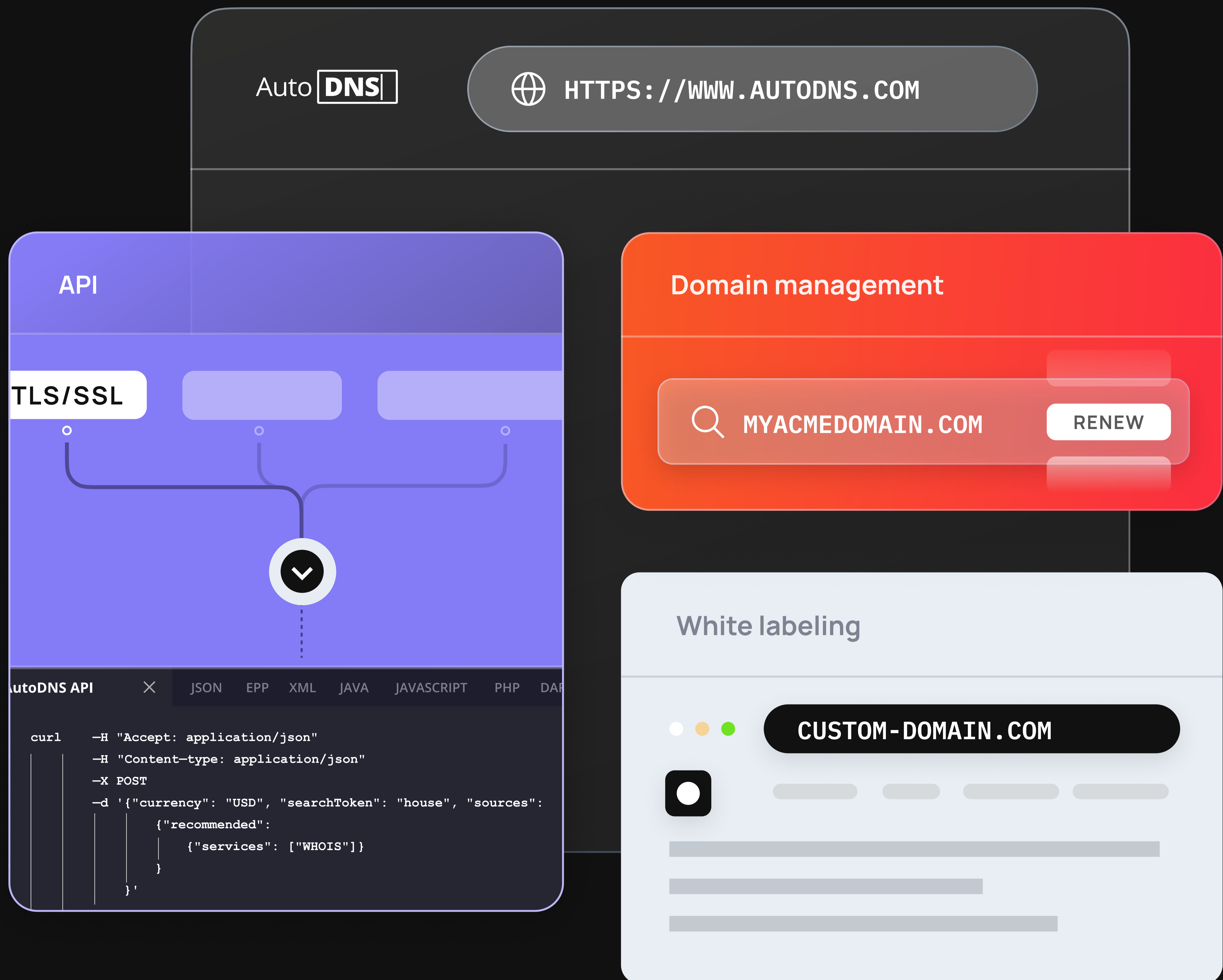
With these efforts I wanted to underscore our role in not only driving growth within our own company but also in fostering success for our partners and advancing the overall domain industry.

[Read the full interview](#) →



Auto **DNS**

Manage domains efficiently. **With AutoDNS.**



InterNetX

Johanna-Dachs-Str. 55
93055 Regensburg
Germany
Phone +49 941 59559-0
Fax +49 941 59559-55
Email: info@internetx.com
www.internetx.com

Explore our Content Hub



Follow us

