Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

DNS4EU: a step change in the EU's strategic autonomy?

Roxana Radu

To cite this article: Roxana Radu (2023) DNS4EU: a step change in the EU's strategic autonomy?, Journal of Cyber Policy, 8:2, 239-256, DOI: 10.1080/23738871.2023.2295937

To link to this article: https://doi.org/10.1080/23738871.2023.2295937

© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 22 Dec 2023.

Submit your article to this journal

Article views: 1554

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=rcyb20

JOURNAL OF CYBER POLICY
2023, VOL. 8, NO. 2, 239–256
https://doi.org/10.1080/23738871.2023.2295937

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

DNS4EU: a step change in the EU's strategic autonomy?

Roxana Radu

Blavatnik School of Government, University of Oxford, Oxford, UK

ABSTRACT

The Domain Name System (DNS) is vital to the internet, enabling everyday uses such as browsing, emailing and chatting. One function in particular – the DNS resolution, performed by resolver operators – allows us to reach what we are looking for online. The market of recursive resolution is highly dynamic and is currently shifting towards open or public resolvers, which tend to belong to large tech companies. In 2022, the European Commission launched the DNS4EU initiative, which established a European resolver as part of the new EU cybersecurity strategy, in order to respond to the resilience, security and privacy needs of the union. This article provides a comprehensive analysis of the DNS4EU project, which provided seed funding to a European competitor in a market increasingly dominated by non-EU players. As a critical infrastructure service, the DNS4EU represents one of the first concrete steps towards enhancing the strategic autonomy of the union. But it also constitutes an unprecedented public intervention in a largely private market relying on voluntary adoption. This article contextualises the DNS4EU initiative, outlining both advantages and limitations of the European strategy and related tender process and implementation plan, concluding with a discussion on the future of DNS resolution.

ARTICLE HISTORY
Received 15 March 2023
Revised 15 November 2023
Accepted 16 November 2023

KEYWORDS
DNS4EU; strategic autonomy; critical infrastructure; European Union; recursive resolver

Introduction

Our online activity and services depend on the Domain Name System (DNS). Human-initiated actions such as web browsing, email and chatting, as well as machine-initiative actions (e.g. running an update) rely on translating domain names, which are easily understandable to us, into numerical IP addresses for computers to take action on. This translation process is called 'DNS resolution'. This function remains invisible to the users, who rely on automatic configurations set by their network provider or their applications[1], with little incentive to change what works relatively well.[2]

The DNS is a critical service infrastructure without which our internet experience would not be the same. It is, however, vulnerable to abuse, misuse and misconfiguration (DNS Abuse Institute 2022; European Commission et al. 2022; Liao et al. 2022). The risks of

CONTACT Roxana Radu roxana.radu@bsg.ox.ac.uk

© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

using the DNS as a vector for attack are key reasons to ensure a secure resolution service. Moreover, internet traffic data holds great monetary value, as does the potential tracking of user behaviour. Since most users never review specific policies applicable to their DNS queries, trust in the resolver operator remains the standard.

As privacy, technological autonomy and digital resilience were raised to the top of the European agenda, the DNS resolution became the centre of attention. The new cybersecurity approach of the European Union (EU) emphasised the necessity for European oversight and capabilities concerning DNS services:

> [P]eople and organisations in the EU increasingly rely on a few public DNS resolvers operated by non-EU entities … [which] renders the resolution process itself vulnerable in case of significant events affecting one major provider, and makes it more difficult for EU authorities to address possible malicious cyberattacks and major geopolitical and technical incidents. (EU Commission 2020, 10)

To address these concerns, the European Commission initiated two tender procedures in early 2022: one for a European cloud and the other for a European resolver (known as DNS4EU). Seed funding for the latter sought to establish a European consortium responsible for running an EU-wide resolution service, designed to respond to local needs and capable of addressing regional cybersecurity threats. It promised to serve public administration, as well as individual users and business actors on the territory of the union, based on voluntary adoption. Due to its scale and ambition, this public intervention was unprecedented. While national protective DNS resolvers exist in a few countries, the EU encouraged the formation of a consortium at the European level. This consortium would then become a competitor in the large and unregulated private market for DNS services, mostly dominated by non-EU tech giants.

This article proceeds as follows: the first part situates the DNS4EU initiative within the domain name resolution market, looking at recent data on key market players and consolidation trends. Section 2 discusses the advantages and disadvantages of public resolvers, as well as public intervention efforts (in the UK and in Canada). The third part traces the process of DNS4EU establishment, from the early days of the tender to the award of the contract, discussing the merits and pitfalls of this strategy. The fourth part examines the role of the DNS4EU in the broader strategic autonomy plans of the EU, zooming in on the competitive advantages it creates. The final section concludes, outlining key opportunities and challenges for this European initiative.

The DNS resolution market: from decentralisation to consolidation

While the DNS itself, as a protocol, remains decentralised in its design and function, the management and operation of DNS infrastructure and services have evolved over time.

What started off as a decentralised system shifted towards centralisation due to the growth of the internet and changes in the market landscape (ENISA 2022a, 2022b; Radu and Hausding 2020). A significant portion of DNS queries are currently handled by a few corporations, which are able to enhance the overall performance and security of the digital services they offer. Given these DNS landscape changes, concerns about DNS privacy and security have become more prominent. Privacy is particularly important as the default DNS protocol is largely unencrypted[3] and subject to many vulnerabilities (Wu 2019).

There are two types of resolution service: free and paid protective DNS. The latter is usually designed and marketed for organisations, whereas the former is more common and addresses a wide range of clients, from individuals to governments. The resolver operators can be local internet service providers, specialised businesses, NGOs or government agencies. An increasingly popular alternative is an open or public resolver, usually made available for free by large corporations to all customer bases.

The DNS was initially designed to distribute the responsibility of managing domain names and IP addresses across multiple entities. This design ensured redundancy and fault tolerance, making the internet more resilient to failures and easier to scale. As the internet rapidly expanded in the late 1990s and early 2000s, the demand for domain names increased significantly. This led to a surge in the number of ISPs and a more distributed approach to domain resolution management. With the rise of national regulations specifically targeting the internet by the end of the 1990s (Radu 2019), local ISPs operating recursive resolvers – free of charge – for their clients, became more susceptible to DNS controls, including blocklists. Governments, cybersecurity agencies and intellectual property organisations resorted to blocklists for a wide number of reasons, from political grounds to copyright infringement and malware prevention.

The offer for an alternative, globally-operating DNS resolver – to use without charge, instead of their default DNS resolution provided by their ISPs – thus appeared as an attractive one. The internet was growing and so was the need for global services and infrastructure. Open resolvers gained popularity worldwide as an alternative to traditional DNS resolution provided by ISPs. The first were run by large-scale DNS providers operating globally, such as Verisign and Neustar. Monetisation strategies varied, with the real-time tracking of user behaviour via DNS queries emerging as a concern (Huston 2022b). At the end of 2009, Google launched its Public DNS service, which was a game changer and remains the most popular resolver globally. Despite the name, public resolvers are mostly private, offered by some of the largest internet companies. Currently, around 20 per cent of the global internet traffic relies on open resolvers. Recent data (Huston 2022b) shows that Google's 8.8.8.8 offering is most popular (16 per cent), followed by Cloudflare's 1.1.1.1 service (2.5 per cent) and OpenDNS (1 per cent). Unlike local ISPs, which are bound by national laws, global providers have long operated outside of local regulatory frameworks applicable in the jurisdiction of the client, giving their recursive resolvers a market advantage.[4] They tend to operate two-sided markets, where services are offered for free to the end users, while the threat intelligence gathered this way is later monetised as part of bigger cybersecurity packages or integrated in their own services for further optimisation (Radu and Hausding 2020).

There is mounting evidence of consolidation around a few powerful players at the level of the DNS (Doan, Fries, and Bajpai 2021; Wang et al. 2021), also mirrored in the resolver market. Measuring the market share of public resolvers using data from the Open Observatory of Network Interference for mobile devices, Radu and Hausding (2020) found that Google and Cloudflare had a dominant position worldwide and were able to acquire a significant part of the market share in a short amount of time. Other studies, relying on different measurements, have found similar trends. Huston and Damas (2022) concluded that open resolvers represent only a third of the total resolution market, but this third goes to four non-European companies, which hold 91.6 per cent of the market share: Google, Cloudflare, 114DNS and OpenDNS. Cloud-based models of DNS resolution are

likely to become even more popular in the future. According to the European Network Information and Security Agency, security concerns represent the primary driver towards public DNS resolvers (ENISA 2022a) and this trend is likely to accelerate in the coming years.

Overall, the shift towards public DNS resolvers is driven by a number of commercial, technical and public policy factors. Large companies may use their existing infrastructure to support DNS resolutions alongside other core services, for example by relying on their large number of data centres around the world, improving the resilience of their systems. Moreover, they may take advantage of existing market shares to include default configurations in browsers and applications and may be in a better position to add encryption protocols and more value-added services (security blocking, parental controls) to choose from. Some exceptions of non-for-profits operating in this space are worth noting, such as Quad9[5] (operating globally) and CIRA's Canadian Shield (for Canadian residents only). The key advantages and disadvantages of public DNS resolvers are discussed in more detail in the next section.

When it comes to policy decisions, DNS blocking and restrictions play a significant role. The 2022 European Network Information Security Agency report on the *Privacy and Security of the DNS* finds the circumvention of DNS blocking to be one of the three major drivers of the shift towards public resolvers, alongside encryption and service outages (ENISA 2022b). Public resolvers operated by global corporations are generally not bound by local regulation and are thus able to resolve names that might be prohibited locally. They tend to be based outside the jurisdiction of the client. Consequently, local access providers may switch to a public resolver to avoid national blocking policies or restrictions, for reasons as diverse as geographically restricted entertainment to politically motivated content censorship.

Despite access and measurement limitations[6], the consolidation of traffic, user data and infrastructure provision into a few private hands is happening faster than initially anticipated. The reverberations of this trend across Europe are significant. The use of public resolvers within the European Union has almost doubled since July 2019 (Huston 2022b). According to an APNIC study using data for January 2022, about 16 per cent of Europeans resort to open resolvers. The same study notes that the patterns of use differ significantly across the European Union, from very low reliance on open DNS resolvers in Belgium, Estonia, Italy and Slovenia, to rates as high as 40 per cent in Malta, 35.8 per cent in Cyprus, and 26 per cent in the Netherlands and Germany. Differences are also visible at the level of usage, as enterprise networks in the EU tend to rely more on public resolvers than individual users (Huston 2022a; ICANN 2022).

Against the backdrop of increased competition for the European market, DNS4EU emerges as a homegrown service aimed at decreasing dependency on foreign providers for a critical infrastructure, reducing vulnerability to outages and offering better security protection and privacy safeguards for EU-based internet users. Importantly, it solves the jurisdictional issues, as neither the resolver providers, nor the data processing, leave the EU. But it remains an intervention into a private market, where the aim is to create a competitor and shape the market conditions for its success.

A closer look at public resolvers: pros, cons and exceptions

Having discussed the evolution of the DNS resolution market, the advantages and disadvantages of shifting to public recursive resolvers become apparent. In this section, the

benefits and limitations of open resolvers are discussed in more detail, with particular reference to user experience and public policy implications.

Some of the key advantages of using open or public DNS resolvers include:

- *Improved performance*. Public DNS resolvers often have a global network of servers strategically located across various geographic regions. This distributed infrastructure helps reduce DNS resolution latency, leading to faster website loading times and improved quality of service.
- *High availability*. Public DNS resolvers are designed to be highly available and redundant. They employ Anycast routing, directing DNS queries to the closest available server, which helps ensure continuous and reliable DNS resolution even in the event of server failures.
- *Enhanced security*. Public DNS resolvers often support DNSSEC (Domain Name System Security Extensions), which helps to verify the authenticity and integrity of DNS data, enhancing DNS security. Moreover, they are managed and maintained by experienced and well-funded teams, ensuring regular updates, patches and service improvement. Additional security measures to help protect users from online threats include blocking access to known malicious websites, preventing users from accessing phishing sites and sources of malware.
- *Privacy and content filtering options*. Some public DNS resolvers, such as those offering DNS over HTTPS (DoH) or DNS over TLS (DoT), provide encrypted communication between users and the resolver. This helps protect DNS queries from eavesdropping and provides an additional layer of user privacy. Additionally, content filtering features allow users to block specific categories of websites, providing control over the types of content accessed at the level of the device (parental controls, etc.).
- *No mandated restrictions*. Public DNS resolvers are independent of internet service providers (ISPs) and do not need to abide by local regulations, allowing users to access DNS resolution services even if their ISP's DNS servers are experiencing issues or restrictions.

Yet features that make them popular choices might also trigger policy concerns. While they are user-friendly and easy to set up, they generally do not operate in the same jurisdiction and regulatory framework as the client. Some of the key limitations of using global open resolvers include:

- *Single point of failure*. The public DNS resolver chosen by a large majority can becomes a single point of failure for DNS resolution. If the resolver experiences issues or downtime, all users relying on it may be affected. At the same time, the global reach of public resolvers may turn them into more attractive targets for their attack surface, despite higher security protections.
- *Centralization*. Cloud computing and content delivery networks (CDNs) include DNS services alongside their other offerings, leading to a centralisation of DNS management within their ecosystems.
- *Privacy and user support concerns*. As many services on our computers use the DNS, there is a possibility of tracking the user activity without their knowledge. While some resolvers claim not to retain identifiable data, the privacy policies of the larger

providers are not always explicit about how the data is collected, used and retained. Current policies used by larger resolver operators may be aligned with the US market, rather than abide by regional or national-level legislation.

- *Public DNS resolvers typically offer no personalized support for individual users.* If issues arise, users may have limited assistance available compared to dedicated technical support from local providers.
- *Data collection and usage*. Public DNS resolvers may log users' DNS queries, which could raise privacy concerns. This data could potentially be shared with third parties or used for targeted advertising. They may also collect and analyse data on users' DNS queries for other purposes, including analytics and research.
- *No Service-Level Agreement (SLA)*. Public DNS resolvers usually do not provide SLAs, which means users have no formal guarantee of the service's performance or uptime. In a similar vein, while there are some privacy and data handling policies published, there is limited transparency over the extent to which information from the resolution service can be integrated into other services (Radu and Hausding 2020).
- *Regulatory and geographic constraints*. Depending on the location and the resolver's policies, some public DNS resolvers may be subject to legal or regulatory restrictions that could affect the service's availability or performance. On the other hand, when national blocking policies and geofencing become more prevalent, cloud-based resolution services can offer appealing alternatives to users for their ability to circumvent restrictions.

Open resolvers for public services

Different models for increased protection for local users already exist around the world, but they constitute the exception, rather than the rule, in a highly concentrated DNS market. The UK's National Cyber Security Centre introduced protective DNS services for governmental agencies in 2017, effectively requiring public administration to switch to a publicly funded DNS resolver. Australia, and more recently the US, has also released similar services, offered free to government entities at the federal and state level. In Canada, a non-profit operates the Canadian Shield resolver open to all individuals and organisations based in the country. Two of these models are discussed in more detail below.

UK's protective domain name service

Since 2017, the UK has its own recursive resolver for public sector organisations, the Protective Domain Name Service (PDNS). The PDNS was developed, and continues to be funded by, the National Cyber Security Centre (NCSC), the UK's technical authority for cyberthreats, as part of its Active Cyber Defence capabilities. In the UK cybersecurity landscape, the NCSC plays a special role, acting 'as a bridge between the UK's industry and government, providing a unified source of advice, guidance, and support on cybersecurity, including the management of cybersecurity incidents' (Infoblox 2022). The PDNS's objective is to secure and protect information technology assets and networks against malware distribution and operation. It is implemented by Nominet UK, the official registry for.uk domain names.

The PDNS is available free of charge to central government and local authorities, as well as emergency services, NHS organisations and the Ministry of Defence. The Cabinet Office has mandated central government departments to use it. It has a Digital Roaming application to allow the redirection of DNS traffic to the PDNS for end users working outside their enterprise networks. While organisations using the PDNS receive metrics about the health of their network, data collected by the resolver helps inform the UK government's cyber incident response (NCSC 2020). The PDNS gathers threat intelligence from all its providers and public sources and applies near-real-time updates to its infrastructure. No filtering – other than for malicious content – is implemented on the PDNS. Although it does not operate the service for private companies, the NCSC has also issued key guidance on the selection and deployment of cloud-based DNS for the private sector (NCSC 2021).

The UK model provided inspiration for a very similar service that the Australian Cyber Security Centre introduced for government entities at the federal and state levels in October 2021. In the US, the CISA released the Protective Domain Name System for all civilian federal agencies in September 2022 (CISA 2022).

Canadian Shield DNS resolver

The Canadian Shield presents a different public resolver model offering free services. It is operated by the Canadian Internet Registration Authority (CIRA), a not-for-profit active for more than 20 years. Available only in Canada, it gives its 3 million users the choice between a private mode (encrypted connection with no filtering), a protected mode (blocking malware and phishing) and a family mode (cybersecurity protections and blocking pornographic content).

The Canadian Shield's policies restrict advertising, tracking and reselling of personal data. Its threat intelligence includes third-party feeds from the open-source community and from commercial technology providers, such as Akamai, which is 'responsible for over 30% of all traffic on the internet and 4% of all global DNS queries' (CIRA 2022). While the threat detection is global, CIRA is in charge of delivering and managing the service from servers located in Canada. CIRA works with the Canadian Centre for Cyber Security to both get, and contribute to, their threat feed, sharing anonymized threat blocking data for research purposes.

The DNS4EU proposal

The public funding offered by the EU for the establishment of a highly distributed and federated recursive DNS resolver operated within the EU builds on the models discussed above. Yet, unlike the two models, it is a first-of-a-kind intervention in a private (and largely unregulated) regional market, altering the competition dynamics by adding a strong local player and defining conditions for its operation on a competitive market. While envisioned to compete with high-performing open resolvers, it would strictly follow European regulations, national restrictions and law enforcement processes. From this perspective, the DNS4EU initiative offers an interesting proposition for a variety of potential customers, from individuals to enterprises and public administrations. The call makes explicit that the current situation is 'especially problematic for public administrations […] who are in need of particularly robust and secure backbone networks and interconnection services such as DNS resolution' (HADEA 2022, 6). In this context, it is

important to note that the EU has not made the DNS4EU usage mandatory for public European institutions, although a high adoption rate is envisioned based on the targeting of multiple consumer bases. Other initiatives in the European space are also voluntary; one such example is the industry-led European Resolver Policy (2021), which offers best practices focused on transparency and privacy.

Establishing a European resolver

When the DNS4EU was initially announced in the 2020 *EU's Cybersecurity Strategy for the Digital Decade*, the commission planned on encouraging the adoption of a DNS resolution diversification strategy among companies, ISPs and vendors in Europe. A financially backed commitment was also envisioned at that stage to support the development of a European alternative that embeds the union's security, data protection and privacy standards. This section discusses the tender process (including its limitations) and the strategy of the winning consortium.

The tender process

By January 2022, when the public call for proposals[7] was out, the Health and Digital Executive Agency of the Commission outlined a two-pronged approach to implementing this vision: (1) to set up infrastructure for a European Cloud (with an allocated budget of €65 million); and (2) to provide seed funding for the establishment of a European DNS resolver service (with a total budget of €14 million). The latter offered seed funding for a European consortium of a minimum of three partners for setting up a resolution service, but not for its operational costs. The part-funding (up to 30 per cent) was intended for an initial period of three years.

Multiple reasons were put forward for issuing this tender: firstly, to provide seed funding for a unified DNS resolver infrastructure for the EU, because the market will not invest in it alone given the lack of a business case (DNS resolution is normally provided free of charge) (HADEA 2022). To strengthen the technological autonomy of the union, additional requirements specify that entities involved in the project must not be controlled from outside the EU. Security sensitive equipment and services used for the delivery of the resolution service had to be produced in the EU.

Secondly, to address the vulnerability concerns that come with the concentration trends in the public resolver market and propose a resilient infrastructure compliant with the latest security and privacy-enhancing standards (HTTPS, DNSSEC), including DNS encryption (e.g. DNS over TLS and DoH) and full IPv6 compliance. Thirdly, to develop a system that is compatible with EU regulations and local concerns and needs of public and private corporate users, and residential internet end users in the EU. In fact, the filtering requirements mentioned in the call were immediately discussed (Cimpanu 2022), prompting Thierry Breton to clarify, on behalf of the commission, that there was no provision for EU-wide network blocking, only filtering for cybersecurity purposes and for purposes specified in national law, already mandatory for resolvers based in Europe (Breton 2022).

With a final deadline set for 22 March (later prolonged to 20 April), the tender triggered a set of immediate reactions from the technical community (Buckridge 2022), not least

because of the brief application window. The consortium building exercise within a short time frame was a challenge in itself. In practice, it meant applicants had to rely on existing partnerships and their own network of contacts, rather than open themselves up to completely new collaborations with a wide range of providers, from threat intelligence companies to open-source software developers and Computer Emergency Response Teams (CERTs). Moreover, the call specifically excluded costs related to operating the infrastructure during its lifetime. As a consequence, despite their eligibility and relevant experience, existing operators of DNS resolution services might have not been incentivized to apply.

The sustainability of the service was a second point of contention. There were questions raised about the business model envisioned, given the three-year limit and partial funding conditions. The tender encouraged the addition of opt-in, paid premium services for enhanced security, tailored to specific sectorial needs. The tender banned the monetisation of personal data, but it did not exclude the use of aggregated data for potential cybersecurity benefits, as long as it was processed in the EU. The sustainability of the project also depended, to a significant extent, on the federated governance structure for the winning consortium. Its members could help reduce costs through shared resources and direct contributions to the establishment. In a short time, they have to ensure the financial resources necessary to cover the operational costs and sustainability beyond the three-year funding cycle.

Last but not least, some worried about the impact of such a significant public intervention in a private market (Buckridge 2022) and that the establishment of the DNS4EU under these conditions would not raise the bar for the whole sector. Quad9, a not-for-profit resolver which operates across Europe, expressed it as follows:

> The tender is singularly funded and does not create circumstances that incentivise adopting these security and privacy enhancements for operators of existing rDNS platforms or services. This approach limits the end-user participation to those who are customers of the consortium members. Other end-users may opt into the service, but that takes time and has a high operational cost, neither provided by the tender. (Quad9 2022)

By the final deadline, only three proposals were received in response to the DNS4EU call (European Commission 2022a), showing that many operators fulfilling the required eligibility criteria had decided against applying. Among the advantages for European users, it is worth mentioning regional resilience, privacy, compliance with modern standards, and jurisdiction-related benefits. Major drawbacks included limited funding and high operational costs for Europe-wide operations.

The winning consortium

In December, the commission announced that the tender contract was awarded to a 13-member consortium (see Table 1) led by the cybersecurity firm Whalebone, headquartered in Brno, Czech Republic. Whalebone, active in network security for large telecoms, ISPs, corporations and government, was legally established in May 2016 and grew to a team size of 80 by 2023. For this project, it partnered with stakeholders across industry, academia and the public sector in 10 EU member states.

With an ambitious plan to protect 100 million people by the end of 2025, Whalebone's CEO Richard Malovic explained that the vision was 'not only to introduce new public infrastructure, but also include the operators in the architecture' (Whalebone 2022). By late

Table 1. DNS4EU consortium members.

Name	Country of origin	Type of entity	Role in the consortium
Whalebone, s.r.o	Czech Republic	cybersecurity company	leader
CZ.NIC	Czech Republic	domain registry (.cz)	member
Czech Technical University Prague	Czech Republic	academic institution	member
Time.lex	Belgium	law firm	member
deSEC	Germany	hosting service	member
Sztaki (in English: Institute for Computer Science and Control,	Hungary	research institute	member
ABI Lab Centro di Ricerca e Innovazione per la Banca	Italy	Italian Banking Association research lab	member
Naukowa i Akademicka Sieć Komputerowa (in English: Research and Academic Computer Network)	Poland	research institute	member
Directoratul Național de Securitate Cibernetică (in English: National Directorate for Cybersecurity)	Romania	public authority	member
Ministry of Electronic Governance	Bulgaria	public authority	associated partner
CESNET	Czech Republic	academic network	associated partner
F-Secure	Finland	cybersecurity company	associated partner
Centro Nacional de Cibersegurança	Portugal	public authority	associated partner

2023, a DNS4EU Stakeholder Group was becoming active, bringing together industry, technical and policy stakeholders to contribute to the development of the project, its long-term sustainability and community ownership.

The proposed implementation for DNS4EU announced by Whalebone is structured along the following pillars:

1. Threat intelligence – from the DNS4EU traffic analysed in real-time to detect, understand and mitigate new threats, as well as regional intelligence exchange, based on cooperation with locals CERTs/CSIRTs and cybersecurity companies.
2. DNS for telcos – building on pillar 1 (threat intelligence) and adding on-premise DNS resolvers, compliant with national regulations and DNS standards.
3. DNS for governments – protective DNS for governments ready to be deployed or customised according to the needs.
4. DNS for users – public and distributed DNS resolvers offered by consortium members, with a transparent privacy policy and optional protective features.

While pillars 1, 2 and 3 of the project would be ready for deployment in 2024, options for end users would only become available in 2025, according to the timeline for the project shared by Whalebone's chief technology officer at an ENISA event in 2023 (Sefr 2023). This sequencing of the project stages reveals the pursuit of two strategic objectives: 1) broader cooperation plans with other significant entities for cybersecurity purposes, in particular local CERTs/CSIRTs and threat intelligence companies; and 2) a prioritisation of the larger market segments for which premium services might also be offered, to ensure the sustainability of the project. Answering a question on the long-term business model, Whalebone

CEO Richard Malovic clarified the vision of Whalebone: 'we believe there is enough market potential to provide monetised services on top of DNS and […] this is a fantastic option to provide public and free accessible services to a large portion of Europeans' (Whalebone 2023b).

If the DNS4EU becomes a main reference in resolution services in Europe in the coming years, it is also due to the complementary actions of the Commission. The revised directive on the security of network and information systems[8] (known as NIS2) – adopted in 2022[9] – specifically targets entities that provide publicly available recursive domain name resolution services for internet end users. In Recital 100, it encourages all stakeholders active within the union to adopt a DNS resolution diversification strategy. Moreover, member states should encourage the development and use of a public and secure European DNS resolver service (NIS2 Recital 100). The scope of the new directive is broader than the 2016 one it replaced, setting a higher bar for cybersecurity risk management and reporting obligations to establish a support mechanism for large-scale cybersecurity crises.

Within the EU, the DNS4EU initiative is aligned with member country regulations, based on the geolocation of the client's IP address. In the newly adopted Digital Services Act, DNS resolvers are designated as mere conduit intermediary services, but they remain subject to orders by national authorities in accordance with national legislation, in compliance with union law, as interpreted by the Court of Justice of the European Union, and in accordance with the conditions established in this regulation (Recital 29).

Prima facie, this set of measures consolidates an agreed vision towards technological autonomy. But at a closer look, the combination of EU-wide rules and member state guidance, reflects deeper, unresolved tensions between European competences and national capabilities and interests. In the words of Martin (2022, 5), 'the division of responsibilities between Member States and the EU's institutions makes a coherent strategy on strategic autonomy very difficult to conceive, and nearly impossible to deliver'. Strategic investments, like the proposed EU Cloud and DNS, thus represent the middle way, prioritising European entities as strong competitors on the regional market. By the same token, the union's industrial strategy also eyes financing for edge computing, high performance and quantum computing, and 6G networks.

Towards strategic autonomy: the DNS4EU initiative in context

When the European Council met to discuss the special measures during the COVID-19 pandemic, it reasserted that '*To be digitally sovereign, the EU must build a truly digital single market, reinforce its ability to define its own rules, to make autonomous technological choices, and to develop and deploy strategic digital capacities and infrastructure*' (European Council 2020, 4). Since then, the EU has been working on various fronts to refine and strengthen its cyber posture. First, underscoring the need to build a resilient, green and digital Europe, Brussels released a new cybersecurity strategy whose objective was to achieve strategic autonomy while preserving an open economy (Consilium 2021). Other key measures mentioned in the 2020 *Cybersecurity Strategy for the Digital Decade* included, among others, a new *Critical Entities Resilience Directive*, the revision of the *Network and Information Services (NIS) Directive*, and the strengthening of the *EU Cyber Diplomacy Toolbox*.

The definition of strategic autonomy dates back to the 2016 EU Global Strategy,[10] but differences in how it is understood by member states persist. In its 2018 State of the Union speech, entitled 'The Hour of European Sovereignty', President Juncker talked about efforts towards 'becoming more autonomous and living up to global responsibilities' (Juncker 2018). At the beginning of the COVID-19 pandemic, Josep Borrell, the Vice-President of the European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, defined strategic autonomy as 'a process, a long-term one, intended to ensure that Europeans increasingly take charge of themselves'. But he also saw it as a process of 'political survival', in which Brussels' capacity to act as a global player comes under challenge. He added that data is at stake for strategic economy, and in particular 'industrial data, and business-to-business data for which there are no satisfactory international regulations' (Borrell 2020).

At a time when digital sovereignty dominates the public discourse in Europe, the question of technological autonomy in a polarised world remains key. The competition over technological models and associated values placed the EU between two poles: the US and China. The geopolitical constraints are key to the understanding of the EU's digital strategic autonomy. Based on a European consultation process, ENISA defined digital strategic autonomy as 'the ability of Europe to source products and services that meet its needs and values, without undue influence from the outside world' (ENISA 2021, 5). Among the early norm entrepreneurs for digital regulation (Radu et al. 2021; Radu and Chenou 2015), the EU has crafted a 'European way' grounded in 'democratic values, respect for the rule of law and fundamental rights' (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2020, 19). This approach was reinforced in the Declaration on European Digital Rights and Principles issued in January 2022 (European Commission 2022b).

However, the large majority of digital infrastructure within European borders is owned and operated by entities headquartered outside of the European Union (Martin 2022). While interdependence has – to a large extent – been built into the internet, the high reliance on non-EU providers has clear implications for the continuity of access to digital services in the region. Such concerns have also been discussed in relation to the roll-out of the 5G mobile infrastructure in Europe (Radu and Amon 2021; Radu and de Gregorio 2023). The DNS service is no exception; while defaults from the local ISPs continue to be preferred by users, the market shares of global open resolvers are steadily growing in Europe – with Google and Cloudflare dominating (ICANN 2022).

Despite a recognition of the growing convergence of views and joint action plans between the EU and the US on technology governance (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2020), the establishment of a European DNS resolver with public funding indicates a break away from the transatlantic dependence. The DNS4EU initiative is part of the broader cybersecurity strategy of the EU, which acknowledges that the consolidation of the resolver market is worrisome for both security and geopolitical reasons. Brussels has recommended a DNS resolver diversification strategy, but has also invested directly in a European alternative, recognising that dependence on non-EU providers could limit EU authorities' capacity to respond in case of crisis (HADEA 2022).

Foreign (non-EU) control checks were a critical part of the eligibility phase of the evaluation of DNS4EU proposals, to ensure that no entities associated with the project

(including as part of the supply chain) would be controlled by third parties. This approach emulates the strategy outlined in the EU Toolbox for 5G networks, where several risk scenarios informed the coordination of mitigation measures at the EU level. Among these, the involvement of high-risk suppliers and the supply chain resilience triggered recommendations to restrict access to sensitive assets and to avoid dependency on particular vendors.

Competitive advantages and limitations

Based on the market conditions set for the European resolver, there are three competitive advantages that are worth analysing, in parallel to limitations and recommendations for action. They relate to the long-term consequences that the project engenders and are significant for the strategic autonomy plans of the European Union. As indicated above, the commission works towards crafting a digital 'European way' under circumstances of geopolitical struggle and rapid changes in technology markets.

Although the proposal was prescriptive about the modern security and privacy standards to which the operators had to adhere, its adoption remained voluntary. An indication of a high adoption rate was, however, expected in the proposal, through the targeting of 'multiple customer bases (e.g. residential, education, governments, and vertical sectors)'. This requires a differentiated and granular approach to privacy, responding to very different needs of the customer base. While the architecture proposed is similar, the various pillars of the DNS4EU proposal (as presented by Whalebone) include both on-premise resolvers for telecommunications operators and protective DNS for governments. In practice, the DNS for governments pillar is built around a ready-made product that can be customised for any country and can be deployed to serve under-protected public organisations such as hospitals and schools (Sefr 2023).

The business model beyond the three-year seed funding is thus significant. While the tender specified that the 'market will not invest in it alone given the lack of a business case (DNS resolution is normally provided for free)', it required a governance structure that would incentivize sharing resources to ensure the long-term sustainability of the project (HADEA 2022, 15). In response, the winning consortium presented a commercial strategy which builds on multiple layers of premium services targeting different audiences: (1) enhanced security layers and integration to existing services available to public institutions and operators; (2) a traffic control app for general public use (including content filtering, parental control, ad blocking, etc.); (3) a threat intelligence platform ready to deliver advanced services to the private sector, including integration to their current services (Whalebone 2023a). At the moment, however, it remains unclear which services are part of the premium offer for governments and public institutions willing to switch to DNS4EU. As the telecommunication and government deployments are planned for 2024, clarifying these elements in a timely manner is highly recommended.

The plans outlined by the Whalebone-led consortium also indicate a regional intelligence exchange focus via cooperation with local CERTs and CSIRTs, as well as commercial entities. A closer relationship with the European threat intel sharing communities would enhance the agility and capacity to respond to cyber incidents as soon as they are detected.

If it has a high adoption rate, the DNS4EU project becomes consequential for the threat intelligence market. Local cybersecurity threats – referred to as 'threats in local language' (HADEA 2022) – are generally underrepresented in commercial threat intel feeds that are dominated by global players. Providing local threat intelligence data that is available and affordable for European ISPs and recursive resolver operators would bring long-term public benefits to the continent, raising the standard of protection for all European users. However, the incentive structure remains underspecified at this stage – competition and scaling challenges need to be considered.

The DNS4EU vision sees engagement with the DNS standardisation community, industry and related stakeholders as important for ensuring the discoverability of the DNS4EU service: on browsers, operating systems and user equipment. It is worth noting that the DNS security standards are unequally implemented across Europe. According to APNIC measurements (APNIC DNSSEC 2022), the usage of DNSSEC validation in the EU ranges from 5 per cent (Romania) to 95 per cent (Finland). With a high rate of adoption for a European resolver that implements all relevant standards, it can be expected that these differences would at least be reduced. Transparency-related discrepancies might also be reduced thanks to the work within the IETF ADD Working Group on publishing resolver information, which can help identify the capabilities of the DNS resolvers (IETF 2023).

Ultimately, a successful DNS4EU initiative has the potential to change the regional DNS resolution market in a relatively short period of time. But would this lead to further consolidation of the market around one European consortium? A continued consolidation towards open DNS resolvers can be expected and DNS4EU will, most likely, reinforce this trend. A realistic scenario involves coexistence of two models of DNS resolution: ISP-provided and public resolvers, serving different purposes and different segments of users in Europe and beyond.

Fast-evolving alternatives are also emerging, calling into question the potential success of the DNS4EU initiative based on voluntary adoption. A recently discussed evolution for DNS resolution is referred to as resolverless DNS (Huston 2022c; Mueller and Sy 2021), where the domain names are resolved on the web server that sends a web page, without needing a resolver. Mueller and Sy (2021) find that there are performance and privacy benefits to this solution, as it does not require additional internet infrastructure such as proxies or DNS resolvers. But this remains disputed on the IETF basic standards and protocols community, in large part due to security considerations and the possibility of further consolidating the power of the few dominant cloud computing companies, by giving control over resolution to the webserver and to the browser.

Conclusion

Largely invisible to the users, the DNS resolution function – performed by resolver operators – has garnered renewed attention from policymakers in recent years. In the European Union, cybersecurity threats and market consolidation dynamics in the Domain Name System have fared high on the agenda of the Von der Leyen Commission, triggering a new set of regulatory measures and competition stimulation actions. The 2022 DNS4EU project combines the ambitions of the new cybersecurity strategy with the EU's efforts to achieve a long-term vision of strategic autonomy for both technology and data assets.

As the tender stated, the main objective of the DNS4EU was to provide high reliability – using a highly distributed and federated structure – and strong protection against global cybersecurity threats and threats specific to the EU. A secondary objective was to address the vulnerability of the DNS resolution process due to dependence on foreign providers and to reduce it by setting the market conditions for an indigenous alternative, which follows EU privacy standards and honours national legislation.

Amid heightened geopolitical tensions, the DNS4EU initiative aimed to decrease dependency on foreign providers by part-funding a European consortium (spanning industry, academia and the public sector) to offer state-of-the-art security and privacy protection for EU internet users. In a highly competitive DNS resolution market shifting power towards non-EU providers, the EU sought an alternative: a public intervention providing seed funding for setting up a public resolver, alongside directions for structuring the market. This analysis outlined the advantages and limitations it created in the process. As a step towards strategic autonomy, the DNS4EU comes into existence at a critical juncture in the evolution of the Digital Single Market and will likely coexist with different models of DNS resolution in the coming years.

Notes

1. Tech-savvy users and enterprise customers could operate a recursive resolver themselves, but that is rarely ever the case, especially on mobile devices. According to some accounts, mobile traffic and desktop traffic are almost equally distributed (Cloudflare 2021).
2. Until service disruptions or outages happen (de Vries et al. 2020).
3. Options to encrypt the DNS queries and traffic, such as DNS over HTTPS (DoH) and DNS over Transport Layer Security (DoT) exist, but they are not uniformly adopted.
4. This is beginning to change as legal proceedings have started against global operators on copyright infringement grounds: Sony Music Entertainment vs Quad9 (Quad9 2023) and Mon Cheri Bridals and Maggie Sottero Designs vs Cloudflare (Brodkin 2021).
5. Quad9 is a public and free open resolver founded in 2016 in California. In 2021, the operation was relocated to Switzerland with a newly-founded Quad9 Foundation, led by a five-member council nominated by non-profits, PCH and SWITCH.
6. It remains difficult to ascertain the accuracy of the market shares, due to complex measurement issues (Huston 2022b; Radu and Hausding 2020).
7. The commission published the tender for *Equipping backbone networks with high-performance and secure DNS resolution infrastructures works* on 12 January.
8. Its full name is *Directive on measures for a high common level of cybersecurity across the Union.*
9. It entered into force on 16 January 2023 and EU member states have 21 months to incorporate its provisions into their national law.
10. Though it has been previously used since 2013 in defence and military documents.

Acknowledgements

The author is grateful for early discussions on this topic with Michael Hausding and for the suggestions and feedback of two anonymous reviewers.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Dr Roxana Radu is an Associate Professor of Digital Technologies and Public Policy at the Blavatnik School of Government, University of Oxford and a Hugh Price Fellow at the Jesus College. Her research focuses on the governance of technology and internet-related policymaking. She often advises governments and international organisations on digital governance issues and serves on the Advisory Group of the EU Cybersecurity Agency. Since January 2023, she is the elected Chair of the Global Internet Governance Academic Network (GigaNet).

ORCID

Roxana Radu http://orcid.org/0000-0002-6329-7820

References

APNIC DNSSEC. 2022. "DNSSEC Validation Rate by country (%)." *APNIC Labs*. Accessed 15 August 2022. https://stats.labs.apnic.net/dnssec.

Borrell, J. 2020. "Why European Strategic Autonomy Matters." *European Union External Action blog*, December 3. https://www.eeas.europa.eu/eeas/why-european-strategic-autonomy-matters_en.

Breton, T. 2022. *Answer Given By Mr Breton On Behalf Of The European Commission.* https://www.europarl.europa.eu/doceo/document/E-9-2022-001306-ASW_EN.pdf.

Brodkin, J. 2021. "Cloudflare doesn't have to Cut Off Copyright Infringing Websites, Judge Rules." *ArsTechnica*, July 10. https://arstechnica.com/tech-policy/2021/10/cloudflare-doesnt-have-to-cut-off-copyright-infringing-websites-judge-rules/.

Buckridge, C. 2022. "DNS4EU: RIPE NCC Open House Discussion." *RIPE NCC Labs* blogpost, January 31. https://labs.ripe.net/author/chrisb/dns4eu-ripe-ncc-open-house-discussion/.

Cimpanu, C. 2022. "EU Wants to Build its Own DNS Infrastructure with Built-in Filtering Capabilities." *Recorded Future News*, January 19. https://therecord.media/eu-wants-to-build-its-own-dns-infrastructure-with-built-in-filtering-capabilities.

CIRA. 2022. "CIRA Canadian Shield – Frequently Asked Questions." *CIRA*. https://www.cira.ca/cybersecurity-services/canadian-shield/faq-public.

CISA. 2022. "CISA Launches its Protective DNS Resolver with General Availability for Federal Agencies." *CISA*, September 27. https://www.cisa.gov/news-events/news/cisa-launches-its-protective-dns-resolver-general-availability-federal-agencies.

Cloudflare. 2021. "Where is Mobile Traffic the Most and Least Popular?" *Blogpost*. October 9. https://blog.cloudflare.com/where-mobile-traffic-more-and-less-popular/.

Consilium. 2021. Cybersecurity Council Adopts Conclusions on the EU's Cybersecurity Strategy. *European Council*, March 22. https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

de Vries, Wouter B., Roland van Rijswijk-Deij, Pieter-There de Boer, and Pras Aiko. 2020. "Passive Observations of a Large DNS Service: 2.5 Years in the Life of Google." *IEEE Transactions on Network and Service Management* 17 (1): 190–200. https://doi.org/10.1109/TNSM.2019.2936031.

DNS Abuse Institute. 2022. *DNSAI Intelligence Report – September 2022.* https://dnsabuseinstitute.org/wp-content/uploads/2022/09/DNSAI-Intelligence-Report-September-2022-FINAL.pdf.

Doan, T. V., J. Fries, and V. Bajpai. 2021. "Evaluating Public DNS Services in the Wake of Increasing Centralization of DNS." *IFIP Networking Conference (IFIP Networking)*, 1–9. https://doi.org/10.23919/IFIPNetworking52078.2021.9472831.

ENISA. 2021. "Cybersecurity Research Directions for EU Digital Strategic Autonomy**.** European Union Agency for Cybersecurity." *ENISA*, April 23. https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy.

ENISA. 2022a. "Why Security Concerns Drive Customers towards Public DNS Resolvers." *ENISA*, February 10. https://www.enisa.europa.eu/news/enisa-news/why-security-concerns-drive-customers-towards-public-dns-resolvers.

ENISA. 2022b. *Security and Privacy of DNS Resolvers. European Union Agency for Cybersecurity Report*. https://www.enisa.europa.eu/publications/security-and-privacy-for-public-dns-resolvers. https://doi.org/10.2824/288837.

European Commission. 2020. *The EU's Cybersecurity Strategy for the Digital Decade. Joint Communication to the European Parliament and the Council*, December 14. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

European Commission. 2022a. "Funding and Tender Opportunities. 21 April update on CEF-DIG-Cloud-DNS Works." https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works.

European Commission. 2022b. "European Declaration on Digital Rights and Principles for the Digital Decade." *European Commission*, January 26. https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. 2020. *Joint Communication to the European Parliament, The European Council and the Council: A New EU-US Agenda for Global Change*. December 2. https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf.

European Commission, Directorate-General for Communications Networks, Content and Technology, I. Paulovics, A. Duda, M. Korczynski. 2022. *Study On Domain Name System (DNS) Abuse*. Brussels: Publications Office of the European Union. https://data.europa.eu/doi/10.2759616244.

European Resolver Policy. 2021. "European DNS Resolver Policy." *European Resolver Policy*. https://europeanresolverpolicy.com.

HADEA. 2022. *Equipping Backbone Networks with High Performance And Secure DNS Resolution Infrastructures*. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/cef/wp-call/2021/call-fiche_cef-dig-2021-cloud_en.pdf.

Huston, G. 2022a. Policy and Technical Considerations, Encrypted DNS Talk. August 8. https://www.youtube.com/watch?v=H4zCR8ZBDtE.

Huston, G. 2022b. "Opinion: DNS4EU." *APNIC blog*, February 11. https://blog.apnic.net/2022/02/11/opinion-dns4eu/.

Huston, G. 2022c. "The path to resolverless DNS." *APNIC blog*, May 17. https://blog.apnic.net/2022/05/17/the-path-to-resolverless-dns/Accessed August 15 2022.

Huston, G., and J. Damas. 2022. Centralization Of DNS Resolution. ICANN presentation, November 15. https://www.icann.org/en/system/files/files/presentation-centralization-dns-resolution-15nov22-en.pdf.

ICANN. 2022. *DNS Resolvers Used in the EU*. Office of the Chief Technology Officer, March 1. https://www.icann.org/en/system/files/files/octo-032-01mar22-en.pdf.

IETF. 2023. "DNS Resolver Information. ADD Working Group. Internet draft, standards track." *Datatracker*, July 3. https://datatracker.ietf.org/doc/draft-ietf-add-resolver-info/03/.

Infoblox. 2022. "The UK's NCSC Recommends Protective DNS for Government and Industry." August 17. https://blogs.infoblox.com/security/the-u-k-s-ncsc-recommends-protective-dns-for-government-and-industry/.

Juncker, J.-C. 2018. *The Hour of European Sovereignty*. State of the Union speech. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en.pdf.

Liao, X., J. Xu, Q. Zhang, and Z. Li. 2022. "A Comprehensive Study Of DNS Operational Issues By Mining DNS Forums." *IEEE Access* 10: 110807–110820. https://doi.org/10.1109/ACCESS.2022.3215753.

Martin, C. 2022. *Cyber Security and European Strategic Autonomy: Coherence and Capability Challenges*. Dublin, Ireland: Institute of International and European Affairs.

Mueller, T., and E. Sy. 2021. "Enhanced Performance and Privacy Via Resolver-Less DNS." 2021 *International Conference on Information Networking (ICOIN)*, *Jeju Island, Korea (South)*: 243–248. https://doi.org/10.1109/ICOIN50884.2021.9334030.

NCSC. 2020. Protective Domain Name Service. Published 17 August 2017, reviewed 27 November 2020. https://www.ncsc.gov.uk/information/pdns.

NCSC. 2021. "Protective DNS for Private Sector: Advice on the Selection and deployment of protective Domain Name Systems (DNS)." *NCSC*, June 9. https://www.ncsc.gov.uk/guidance/protective-dns-for-private-sector.

Quad9. 2022. "DNS4EU – Quad9 Perspective and Status." *Quad9 blogpost*, February 21. https://quad9.net/news/blog/dns4eu-quad9/.

Quad9. 2023. "Quad9 And Sony Music German Injuction Update For July 2023." *Quad9 blogpost*, July 4. https://quad9.net/news/blog/quad9-and-sony-music-german-injunction-update-for-july-2023/.

Radu, R. 2019. *Negotiating Internet Governance*. Oxford: Oxford University Press.

Radu, R., and C. Amon. 2021. "The Governance of 5G Infrastructure: Between Path Dependency and Risk-Based Approaches." *Journal of Cybersecurity* 7 (1): 1–16. https://doi.org/10.1093/cybsec/tyab017.

Radu, R., and J.-M. Chenou. 2015. "Data Control and Digital Regulatory Space(s): Towards a New European Approach." *Internet Policy Review* 4 (2): 1–10. https://doi.org/10.14763/2015.2.370.

Radu, R., and G. de Gregorio. 2023. "The New Era of Internet Governance: Technical Fragmentation and Digital Sovereignty Entanglements." In *Hybridity, Conflict, and The Global Politics of Cybersecurity*, edited by F. Cristiano, and B. van den Berg, 15–30. London: Rowman & Littlefield.

Radu, R., and M. Hausding. 2020. "Consolidation in the DNS Resolver Market: How Much, How Fast, How Dangerous?" *Journal of Cyber Policy* 5 (1): 46–64. https://www.tandfonline.com/doi/full/10.108023738871.2020.1722191.

Radu, R., M. Kettemann, T. Meyer, and J. Shahin. 2021. "Normfare: Norm Entrepreneurship in Internet Governance." *Telecommunications Policy* 45 (6): 1–7. https://doi.org/10.1016/j.telpol.2021.102148.

Sefr, R. 2023. *DNS4EU: Scope and Timeline*. Whalebone. https://www.enisa.europa.eu/events/1-dns4eu-project-overview-enisa-1.pdf.

Wang, Synthia, Kyle MacMillan, Brennan Schaffner, Nick Feamster, and Marshini Chetty. 2021. "A First Look at the Consolidation of DNS and Web Hosting Providers." *Cornell University*, October 28. https://arxiv.org/abs/2110.15345.

Whalebone. 2022. Press Release: DNS4EU. December 20. https://www.whalebone.io/post/press-release-dns4eu.

Whalebone. 2023a. "DNS4EU." *Whalebone*. https://www.whalebone.io/dns4eu.

Whalebone. 2023b. DNS4EU Online Press Conference. January 10. https://www.youtube.com/watch?v=Lj8ePGKfQtM&t=19s.

Wu, P. 2019. "DNS Encryption Explained." *Cloudflare blog*, October 29. https://blog.cloudflare.com/dns-encryption-explained/.