

Impact of the proposed NIS2 Directive in relation to organisations self-managing their domain name service

Executive Summary

The proposal for the revised Directive on Security of Network and Information Systems (draft NIS 2) inadvertently makes many organisations in both the private and academic sector subject to a regulatory regime for ‘essential services’. The draft directive, aiming to improve the cybersecurity posture and risk management of organisations that provide essential and important services to the economy and society, includes in its definition of ‘essential’ entities of the Digital infrastructure all DNS service providers that provide ‘authoritative’ name resolution for domain names.

The intent of the draft Directive, substantiated by the *Impact Assessment* that accompanies the proposal, is to ensure that root and top-level domain name services, as well as DNS service provided as a business offering by domain name registrars and web hosting companies, are all brought to a similar, high common level of cybersecurity across the Union.

However, the way ‘DNS service provider’ is defined in the NIS2 draft, combined with the exclusion of *specifically* DNS service providers from both the size-cap criterion and from any considerations of their economic and societal impact, *inadvertently* brings a very large number of non-important entities within its sway. Many organisations, both in the private sector as well as in academic and research establishments, operate *their own* authoritative domain name resolution services for their own domain names. Incidents affecting these domain name services impact only that entity itself and have little impact of the type the Directive is intended to address. They themselves rely solely on the domain name services of their chosen ccTLDs, and the internet end-users can reach them either directly or through any *recursive* domain name resolution services that the end-user may have opted to use.

By not distinguishing between ‘recursive’ and ‘authoritative’ domain name resolution services in the definition of ‘DNS service provider’ in Article 4 (14), the proposed Directive *does* ‘bring considerable changes in terms of coverage of entities’, contrary to what is stated in the *Impact Assessment*, by including large numbers of organisations in the Union that operate their domain name servers themselves for otherwise non-essential and non-important entities – ranging anywhere from soup brands to physics research data. By not excluding natural persons from the definition of ‘entity’, it even includes unquantifiable numbers of individual computer enthusiasts. The classification of DNS service providers as ‘essential entities’ moreover incurs the overhead of the most stringent regime (under Art. 29), incurring a heavy and unexpected burden *not only* on the organisations involved, *but also* and specifically on ENISA and on the supervisory authorities in the member states.

To ensure that only those entities *intended* to be in scope of the NIS2 Directive are included, either:

- the definition of ‘DNS service provider’ in Art. 4 (14) could be augmented by clarifying it applies to entities that provides *authoritative* domain name resolution *as a service procurable by third-party essential and important entities*; or
- Article 2(2)(a)(iii) could be scoped specifically to ‘top-level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I ‘... *that provide recursive domain name resolution services*’, thus making providers of solely *authoritative* DNS services subject to a qualifications based on Art. 2(2)(b) – (g), where also the number of domain names hosted by the service could be part of the considerations.

Table of Contents

Executive Summary	1
Introduction and context.....	2
DNS service providers in the draft Directive	4
An unintentional impact with large consequences	4
Conclusion and proposed resolution.....	7
Acknowledgements	7
Colophon	7

Introduction and context

The European Commission, on December 16th 2020, adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive)^{1,2}. It changes the perspective on security and incident management for essential and important societal services with respect to the existing (2012) NIS directive, by taking a systemic approach in addressing threats to the digital society. Quoting the Commission: “*Now any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market*”³.

In order to achieve the intended systemic effects, more entities are brought within scope of the directive. Whereas hitherto operators were classified within specific sectors essential to society, or as digital service providers, the NIS2 draft Directive abolishes that distinction, providing ‘a list of sectors and types of services where the entities falling within the NIS scope would be ‘essential’, and a respective list of sectors and types of services for ‘important’ entities’⁴. It acknowledges that operators of essential services ‘are dependent on certain digital service providers, such as cloud service providers, which makes the latter as important or essential as the former and hence requires a similar regulatory regime’⁵.

Managing these interdependencies in the network is very important for the assessment of cybersecurity risks and establishing trust. During the actual mitigation of security incidents the ability to contact all relevant actors and collaborate is similarly crucial. This is reflected in the new way in which the draft Directive sets its scope of ‘essential’ (Annex I) and ‘important’ (Annex II) services, and what kind of entities are included in each of them. For Annex I⁶, this includes the obvious societal necessities like energy, transport, finance, health, drinking and waste water management, public administration, and space. It also includes the “Digital Infrastructure” (8.)

The definition of the kind of ‘essential entities’ included in *Digital infrastructure* has been significantly extended in the draft Directive, and besides ‘Cloud computing service providers’ now also includes

¹ <https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union>

² “Draft NIS2 Directive”, Proposal for a Directive [...] on measures for a high common level of cybersecurity across the Union, COM(2020) 823 final, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

³ Ibid. Draft NIS2 Directive, recital (20).

⁴ Commission Staff Working Document: *Impact Assessment Report* SWD(2020) 345 final, <https://ec.europa.eu/digital-single-market/en/news/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union>, pg. 57

⁵ Ibid., *Impact Assessment Report* SWD(2020) 345 final, pg 57

⁶ https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72172

Internet Exchange Point providers, data centre service providers, content delivery networks, and top-level domain registries.

Significantly, also “DNS service providers” are included in the definition of *Digital infrastructure*. The Impact Assessment clarifies the intent and purpose of including them as ‘essential services’:

In order to ensure that small or micro entities which are nevertheless of critical importance for the societal or economic activities are not left out of the NIS scope, exceptions to the size-cap rule would be established.

[...]

(iv) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact,

[...]

“Top-level domain name registries and domain name system (DNS) service providers would also be excluded from the size-cap rule.”⁷

Singling out top-level domain name registries and the (ccTLD) DNS service they provide explicitly is obviously merited, given that incidents at this level have national or (for ‘.eu’) Union-wide effects.

The “large number of domain name registrars and web hosting companies” are also specifically included, with footnote 177 that these “offering authoritative DNS resolution as part of their domain registration services”. Given that most domain name registrars offer their services to all takers, and that therefore *also* entities providing essential or important services could be reliant on the authoritative DNS service offered by these registrars or web hosting companies, including those that publicly offer such authoritative DNS services – regardless of their size – could be well warranted.

One type of DNS service is not discussed in the Impact Assessment, nor anywhere in the draft Directive and ancillary documents: those non-essential and non-important entities that – having configured their domain name by adding their name servers in the ccTLD domain, proceed to operate the authoritative DNS service for that domain entirely themselves. The integrity and availability of their domain name resolution depends on nothing more than the ccTLD DNS service and their own, local, self-managed infrastructure. No other parties are involved in service provisioning. Internet end-users and other, recursive, DNS service providers deal directly with the authoritative domain name service owned and operated by the organisation itself.

Such ‘self-managed DNS’ organisations, apart from having some knowledgeable ICT staff, never intended to be a “Digital infrastructure”. Nor is it, merely by operating its own authoritative DNS server, suddenly of an essential nature to the economy or to society.

As currently worded, it has an even more unexpected effect: since *natural* persons are included explicitly in the definition of ‘entity’ (Art. 4 (24)), also any individual computer enthusiast running a personal or family domain using a domain name server at a private home, in a makerspace, or at a friend’s place (thus even providing the redundancy common required by ccTLD operators), is a “DNS service provider” in the current definition – and consequently has to register with ENISA and is subject to the Art. 25 regimen for supervision! It appears unlikely that ENISA or national supervisory authorities would welcome such an unquantifiably-large number of hobby-computer enthusiasts.

The Domain name system is justly described in the Impact Assessment as “a hierarchical distributed naming system which allows end-users to reach services and resources on the open internet”⁸. The leafs of the hierarchy are single domains owned by organisations and natural persons, that often can and do hold up their own in terms of ICT services.

⁷ Impact Assessment Report SWD(2020) 345 final, pg. 60-61.

⁸ Impact Assessment Report SWD(2020) 345 final, pg. 5

DNS service providers in the draft Directive

The draft NIS2 Directive released on December 16th states in Recital (15):

Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

This emphasises the “integrity of the internet” and the dependency of the digital economy and society thereon, and then proceeds that it should apply to “authoritative servers for domain names” - without further qualifying this statement. However, in view of the discussion in the *Impact Assessment* and given the aim of the NIS2 Directive, not all leafs of the DNS hierarchy are equally important.

The definitions in Article 4 (14) also include the all-encompassing description of the DNS service:

‘DNS service provider’ means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;

However, with such a broad definition of “DNS service provider” as stated in the draft Article 4 (14), the scope of the directive is unexpectedly widened to include also any ‘leaf’ authoritative domain name resolution service operated by any self-managed organization, regardless of the nature or size of such organisation (Art. 2(2)(a)(iii):

2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:

(a) the services are provided by one of the following entities:

[...]

(iii) top-level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;

Inadvertently, by combining the overly-broad definition of ‘DNS service provider’ with the blanket inclusion of *specifically* ‘domain name system (DNS) service providers’ through Art. 2(2)(a)(iii), *all* entities that run their own authoritative domain name server, regardless of their size, regardless of their nature or criticality to the economy, to society, or to the digital infrastructure as a whole, are brought in scope of the NIS2 Directive.

An unintentional impact with large consequences

The draft Directive as written thus makes the implicit assumption that operating a domain name resolution service only and exclusively happens as part of domain name registration or web hosting. Both the draft Directive and the Impact Assessment⁹ accompanying it, fail to acknowledge the common practice whereby organisations, having registered a domain name with a top-level (country) domain name register (ccTLD operator), run their own, self-managed, authoritative DNS service to resolve those domain names that they own and manage themselves.

Organisations thus responsible for their own DNS name service are common, both among larger private enterprises, and in organisations otherwise availing over their own in-house digital expertise,

⁹ *Impact Assessment Report SWD(2020) 345 final*

such as academic and research establishments. Yet these are not, by their scope or societal impact, ‘essential’ or ‘important’ entities in the ‘DNS resolution chain’, as intended by the draft Directive. For example, prominent enterprises of the first group include¹⁰ Unilever and its brands (like “knorr.de” for soups and ready-made meals), Skoda (“skoda.cz”), Ferrari (“ferrari.it”), or the Swedish Sandvik tools company (“sandvik.se”). The entities with in-house expertise also include large numbers of universities and research institutes that operate authoritative DNS services for the domains they own themselves, research labs such as Nikhef (“nikhef.nl”), CERN (“cern.ch”), or ESRF Grenoble (“esrf.fr”), and universities throughout Europe.

It is self-evident that the societal impact of unavailability of such a domain is limited, and its effects are non-systemic in any way. A failure of their DNS service provision would solely and exclusively impact *only their own organisation and domains (brands)*, and it does not have any systemic impact.

Yet, by being a DNS service provider – for their own domains - , they are brought under the scope of the directive by being listed in Annex I (‘essential entities’) sub 8 and classified as “Essential entities”. In addition, this scope is not constrained by the size-cap rule, which inadvertently does not apply since *any* DNS service provider is explicitly brought in scope because of Art. 2(2)(a) sub (iii).

But the temporary inability to view a page on soup, or the specifications of a new Ferrari, or the results of a scientific experiment, obviously has negligible societal impact.

From the Impact Assessment¹¹ it is clear that the *intention* of the directive is addressing providers of DNS services for whom operating DNS services is part of their business:

*For digital infrastructure, options 3 does not appear to bring considerable changes in terms of coverage of entities. In particular, 173 such entities were identified as OES by the Member States, while there are: 28 major country-code top-level domain (ccTLD); [...]; for authoritative DNS resolution: two root name servers, 28 major ccTLD entities and a large number of domain name registrars and web hosting companies, [...]*¹².

where the ‘large number of domain name registrars and web hosting companies’ run (authoritative) DNS services that anyone can procure, and often host tens of thousands to millions of domain names. For such providers, incidents affecting the DNS service will impact a large number of customers – *i.e.*, have an effect not only on their own organisation – and thus *could* have impact on public safety, public security or public health (Art. 2(2)(d)) or induce a systemic risk (Art. 2(2)(e)).

Yet organisations operating *their own* DNS service were clearly not considered in the impact assessment, nor consulted, nor considered when drafting the definition of “DNS Service Provider” in article 4 (14) of the draft directive:

*‘DNS service provider’ means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers*¹³;

¹⁰ List of samples compiled on January 6th, 2021, based on then-current data from the country-level TLD registries. Listed companies have at least one of their name servers pointing to internet addresses that they administer themselves, based on RIR internet address databases. Some, like Unilever, Skoda, and Sandvik, exclusively use their own servers and have no external secondary servers.

¹¹ *Impact Assessment Report SWD(2020) 345 final*

¹² *Commission Staff Working Document, Impact Assessment Report SWD(2020) 345 final, page 62*

¹³ Draft NIS2 directive, Article 4 “Definitions”, (14).

An organisation-specific, 'self-managed', authoritative DNS service *ipse facto* has to provide 'domain name resolution service' to 'other DNS service providers' (specifically to recursive DNS resolvers¹⁴) as well as "end-users", in order for the end-users to resolve that one company's own domain names!

But the organisation's DNS service need *not* be run at a name registrar (name registration is a function quite separate from DNS service provision), nor at a web hosting company (which likely is not involved at all, because the internet and DNS are not exclusive to web content, and neither does an organisation become a 'web hosting company' merely by running its own web site).

The wording of the definition of 'DNS service provider' in Article 4 (14) is thus too broad and goes beyond its stated intent and impact. For organisations self-managing their authoritative DNS service, 'option 3' (the NIS2 draft Directive) **does** 'bring considerable changes in terms of coverage of entities'. Tens of thousands, if not more, of organisations, small and large, and even regardless of the size-cap for SMEs, suddenly find themselves drawn into scope - merely because they operate their own authoritative DNS server for their own domains. It even draws in individuals that are computer enthusiasts and run their own authoritative service for their home or family domains.

That does not mean that the organisations affected are specifically at risk for cybersecurity incidents in their DNS service; their services are commonly resilient by design and highly available.

Organisations are already incentivised to design and operate their service in this way, both by implicit requirements from the ccTLD¹⁵ operator (that typically insists on service redundancy), as well as of their own volition, given that the pain for their own organisation is much larger than the broader societal impact. The NIS2 draft Directive would not change that nor improve cybersecurity posture, but only add administrative burdens to entities that are not otherwise either 'essential' or 'important'.

The impact assessment does not consider the significant administrative and regulatory overhead thereby imposed on organisations that were hitherto not subjected to the NIS directive, and that were not intended to be subject to NIS2, but are now inadvertently brought into its scope. Furthermore, with 'DNS service providers' classified as 'essential' entities under Annex I (8), all these entities, private and academic alike, would become subject to more intense 'Supervision and enforcement for essential entities' under Art. 29 – just as a result of operating their own authoritative DNS service.

Similarly, this inadvertent inclusion creates a considerable and serious load on both national supervisory bodies and on ENISA, where all these entities have to register themselves, and who will have to process and forward their information to the single points of contact in the member states.

The competent authorities in each member state also have to bring the highly resource- and administration intensive regime for 'essential entities' (Art. 29) to bear on all these otherwise non-essential organisations, resulting in wastage of resources that could have been spent more rewardingly in improving the cybersecurity posture of truly essential entities.

¹⁴ "[...] recursive DNS resolution: DNS resolvers provided by most internet service providers and by third parties, mostly large global technology companies located outside the EU." *Impact Assessment Report* SWD(2020) 345 final, page 62

¹⁵ Country-level top level domain operators have long since required that at least two idempotent authoritative name servers are provided during domain name registration. Many self-managing organisations ensure those are geographically distributed, and – between academic and research establishments in particular – add cross-border mutual 'secondary' servers that further improve reliability. Many private enterprises similarly ensure reliability by operation of off-site, external, authoritative domain name resolvers for their domains.

Conclusion and proposed resolution

The draft NIS2 Directive, as currently written, inadvertently includes organisations that self-manage their domain name resolution services in the definition of “DNS Service Provider” in Art. 4(14), even if such entities are not essential or important as meant in the NIS2 draft Directive, and would not otherwise be considered in scope. Such organisations, which exist in large numbers in both the private and academic sector, were not considered in the Commission’s Impact Assessment. Inclusion of these organisations would place an undue burden both on the regulatory bodies involved (because of the increased number of organisations subject to it) as well as on the organisations themselves (in terms of having to deal with the *ex ante* registration and supervisory regime).

In order for the Directive to achieve its intended effect, the existence of self-managed DNS service provisioning must be acknowledged. The smallest textual change could be a change of definition of “DNS Service Provider” of Article 4 (14) of the draft NIS2 directive. Where it currently states

(14) ‘DNS service provider’ means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;

this definition may be used to clarify that organisations that self-manage their DNS service are not included in the scope of “DNS service provider”, for example by updating the definition to read:

*(14) ‘DNS service provider’ means an entity that provides recursive domain name resolution services to internet end-users and other DNS service providers, or an entity that provides authoritative domain name resolution **as a service procurable by third-party essential and important entities**;*

A more robust solution compatible with intent could be to limit the applicability of Art. 2 (2)(a)(iii) to only top-level domain name registries and ‘[...] *those domain name system (DNS) service providers referred to in point 8 of Annex I that provide recursive domain name resolution services*’. Those providers of *authoritative* DNS services that are of systemic value to the digital infrastructure will then nevertheless be covered under the criteria of Art. 2(2)(b) – (g). The possibility to designate specific authoritative DNS service providers as ‘essential’ is thus retained.

Alternatively, a threshold value for the number of domains managed by the DNS Service Provider could be considered in the definition, or in Art.2 (2) itself. For example, only authoritative providers with more than 100.000 domains registered to entities in any single member state, could be made to fall within the qualifying definition.

In this way, the intended effect of reducing the impact of incidents on public safety, public security or public health (Art. 2(2)(d)) and the reduction of systemic risk (Art. 2(2)(e)) is ensured, in a way fully acknowledging the scope of DNS service providers as given in the Impact Assessment.

Acknowledgements

We want to profoundly thank Andrew Cormack (JISC) both for bringing the NIS2 to our attention¹⁶ and for the subsequent insights and discussions on scope and applicability of NIS2 to organisations operating their own authoritative DNS servers which have been inspirational for this text. Needless to say, any and all errors, inconsistencies, misrepresentations, and opinions are entirely my own.

Colophon

David Groep, Nikhef, Amsterdam, January 2021. E-mail: davidg@nikhef.nl.

This document can be freely distributed under the CC-BY-4.0 license.

¹⁶ <https://regulatorydevelopments.jiscinvolve.org/wp/2021/01/05/whois-access-and-the-nis2/>