The EU NIS-2 proposal and the DNS

David Clark

August 2022

A working paper of the CAIDA GMI3S project.[1]

1 Summary

This note summarizes the potential impact on the Internet Domain Name System from the proposed revision of the European Union's Network and Information Security (NIS) Directive.[2] The European Union NIS-2 Directive replaces the original network and information systems (NIS Directive) from 2016, to account for (among other things) the changing character of the digital society and the increased need for improved cybersecurity. Quoting the directive:

> *The NIS Directive is not sufficiently clear when it comes to the scope for operators of essential services and its provisions do not provide sufficient clarity regarding national competence over digital service providers.*

The directive imposes general requirements on providers of network and information services, if deemed *critical* or *important* (Section 11), including vulnerability reporting, risk assessment, operating their systems at a level of security consistent with assessed risk, and attention to supply chain issues and third-party relationships. The legislation also imposes specific obligations on providers of DNS services in the EU (including registries and registrars) to maintain complete and accurate registration data (sometimes known as "Know Your Customer" or KYC obligations), and share this data in a timely manner to "legitimate access seekers". Some smaller providers are exempt, but providers of electronic communications networks or of publicly available electronic communications services, trust service providers, and Top-level domain name (TLD) name registries are obligated under this legislation, independent of size. This memo examines the sections of the Directive that relate to DNS operation and security.

2 History

We assume that readers of this memo are familiar with the issues surrounding access to DNS Whois data, the presumed barriers to release of DNS Whois data created by the EU GDPR, the process ICANN established to resolve this issue (the Temporary Specification), and the frustration of many parties (most specifically those concerned with DNS-enabled illicit activities) with the unresponsiveness of many DNS registrars and registries in providing access to Whois data, even when the data in question is not protected by the GDPR.

In February 2020, the European Parliament sent a Parliamentary Question (a formal query) asking the Commission (in essence) what steps it intends to take to resolve this issue.[3] While the NIS-2 Directive

[1]This material is based on research sponsored by the National Science Foundation (NSF) grant OAC-2131987. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of NSF.

[2]"The NIS2 Directive: A high common level of cybersecurity in the EU", `https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333`

[3]"Lack of access to WHOIS internet domain registration data", `https://www.europarl.europa.eu/doceo/document/E-9-2020-000826_EN.html`.

does not discuss the specific forces that led to its drafting, it is reasonable to assume that it reflects the Commission's attempt to respond to this question (and other calls for better access), and establish rules to ensure that access to DNS Whois data is available to legitimate parties in the EU on a timely basis.

3 Organization of the Directive

The Directive has three parts. The first is a brief summary of its articles, background, and the authority of the EU to issue the Directive. The second is the justification for and objectives of the Directive. Grammatically, the sections begin "Whereas". The third part is the proposed legislation, which is in many ways more terse than the *sections* in the Directive, and is organized as a series of "Articles", with numbered paragraphs within each Article. This memo quotes from both the sections in the Directive, and the articles in the actual proposed regulation. All quotes are from the Directive. The text is often indirect, because it does not directly regulate, but instead imposes requirements on Member States to implement conforming regulations.

4 Scope of the NIS-2 Proposal

The Directive identifies two classes of regulated entities: those offering *essential* services and those offering *important* services. (Section 11.)

> *Depending on the sector in which they operate or the type of service they provide, the entities falling within the scope of this Directive should be classified into two categories: essential and important. That categorisation should take into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services. Both essential and important entities should be subject to the same risk management requirements and reporting obligations. The supervisory and penalty regimes between these two categories of entities should be differentiated to ensure a fair balance between requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.*

The Directive exempts smaller providers from the regulations:

> *The proposal foresees a general exclusion of micro and small entities from the NIS scope and a lighter ex-post supervisory regime applied to a large number of the new entities under the revised scope (so-called important entities).*

However, there are relevant exceptions:

> *Micro and small entities ... are excluded from the scope of the Directive, except for providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD) name registries and public administration, and certain other entities, such as the sole provider of a service in a Member State.*
>
> *As a rule, essential and important entities are deemed to be under the jurisdiction of the Member State where they provide their services. However, certain types of entities (DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers, as well as certain digital providers) are deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.*

5 Obligations of entities providing essential & important services

The Directive lists the following obligations for entities that provide essential and important services.

- Vulnerability reporting: a number of sections discuss this objective.
- Risk-management: measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact.
- Section 42: "Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it."
- Section 43: Supply chain. "Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures."
- Section 45 "Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular."

5.1 Relevant text of the regulation

These are the Articles relevant to the obligations of entities providing essential and important services:

Article 18
Cybersecurity risk management measures

1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

2. The measures referred to in paragraph 1 shall include at least the following:
(a) risk analysis and information system security policies;
(b) incident handling (prevention, detection, and response to incidents);
(c) business continuity and crisis management;
(d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
(f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;
(g) the use of cryptography and encryption.

Article 21
Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.

6 Internet

The Internet is mentioned in many places, and is implicit in many sections. The most specific mention is:

- Section 51: "In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto."

7 Provisions specific to the DNS

From the summary:

> TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data. Furthermore, such entities are required to provide efficient access to domain registration data for legitimate access seekers.

The regulation does not appear to provide a definition of "legitimate access seekers."

The article that scopes the DNS regulations is as follows:

Article 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.[4]

The relevant sections of the proposal are as follows:

- Section 59: "Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law."
- Section 60: "The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, (CSIRTs, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data."
- Section 61: "In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data.

[4]ICANN, in comments they provided to the EC on NIS-2, expressed the opinion that the scope as written was over-broad, and in particular that small providers of recursive name service and authoritative name service for services that themselves were not essential or important should not be within the scope of this regulation. "ICANN org comments on the Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the EU, repealing Directive (EU) 2016/1148 (NIS 2 Directive)", https://www.icann.org/en/system/files/files/icann-org-comments-proposed-nis2-directive-19mar21-en.pdf

In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules."

- Section 62: "TLD registries and the entities providing domain name registration services for them should make publically available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board."

- Section 64: "In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings."

- Section 65: "In cases where a DNS service provider, TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider and digital provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether it is apparent that the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the entity is established, is as such insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate

of the entity to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting."

7.1 Relevant text from the regulation

Article 23

Databases of domain names and registration data
1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.
2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.
3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.
4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.
5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Article 24
Jurisdiction and territoriality

1. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.
2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union.
3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Directive.
4. The designation of a representative by an entity referred to in paragraph 1 shall be without prejudice to legal actions, which could be initiated against the entity itself.

8 Definitions

(9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;
(13) 'domain name system (DNS)' means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet;

(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;

(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers;

9 Additional articles

Several other Articles seem somewhat relevant to the regulation of the DNS.

CHAPTER V
Information sharing
Article 26
Cybersecurity information-sharing arrangements

1. Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:
(a) aims at preventing, detecting, responding to or mitigating incidents;
(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.

5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:
(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;
(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity. These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

10 Research

The role of academic research comes up in the document in two places. One is section 45, quoted above. The other is:

Article 2

(f) [Member States shall in particular adopt] "a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure"

11 Essential and important services

The following are identified as *essential* services in the telecommunications sector (See Annex 1):

- Internet Exchange Point providers
- DNS service providers
- TLD name registries
- Cloud computing service providers
- Data centre service providers
- Content delivery network providers
- Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014(25)
- Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972(26) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available

The following are identified as *important* services in directive:

- Providers of online marketplaces
- Providers of online search engines
- Providers of social networking services platform