THE NETWORK INFORMATION SYSTEMS DIRECTIVE (EU) 2016/1148: INTERNET SERVICE PROVIDERS AND REGISTRIES

Domenica Bagnato[1]

DOI: 10.24989/ocg.v.338.9

Abstract
The NIS Directive [1] defines critical infrastructures and operators of essential services. It also calls for organizational measures to ensure these infrastructures are protected from cybercrime and terrorism. This also includes the establishment of a national framework for emergency response. The list of essential services in Annex II does contain certain elements of Internet infrastructures, such as Domain Name Servers and Internet Exchange Points. However, in a truly remarkable omission, the Directive does not include Internet Service Providers (ISP) [2]. Since operators of essential services are subject to stringent security requirements, it would be helpful to include them as operators of essential services. This seems even more appropriate as many other Annex II infrastructures, such as banking, health and transport, heavily rely on a working Internet infrastructure, which is largely dependent on ISPs.

This paper discusses the omission in the NIS Directive of the ISPs and the incomplete list and co-dependent registries namely, the IP address space registry and the Autonomous System registry and their necessity in supporting the root Domain Name System.

1. Network Information Systems Directive (NIS)

On the 6th of July 2018, the Network Information Systems Directive (EU) 2016/1148, referred to in this paper as the NIS Directive, was passed by the European Parliament and the Council of the European Union.[2] The NIS Directive formulates a defence strategy against an impending threat to critical infrastructure concerning the EU Member States, namely cyber-attacks. The word "*concerning*" highlights the fact that not all critical infrastructure particularly digital infrastructure pertaining to the Internet may be located in the EU Member State region.

2. Internet Service Providers (ISP)

Loosely speaking, an ISP provides individual internet users or organisations, with their own private networks including servers and routers, with Internet access. RFC 1930 defines an Autonomous System (AS) as:

*"a **set of routers** under a **single** technical **administration**, using an **interior gateway protocol** and common metrics to route packets within the AS, and using an **exterior gateway protocol** to route packets to other ASes."* (my emphasis) [3]

[1] Domenica Bagnato, Managing Director, Hierodiction Software GmbH. Email: domenica.bagnato@hierodiction.com
[2] [1] In the following, "Directive" or Recitals or Articles without further reference will refer to [1].

Technically speaking, an ISP is an instance of an "autonomous system" (AS), as defined in RFC 1930, that connects other ASes and end users to the Internet.
In the following, this functionality is discussed to provide an overview of what is involved but also the design choices a possibly updated Directive has to face. Two factors also have to be taken into account:

- ISPs (an instance of an AS) are sometimes not directly responsible for all the infrastructure discussed below;
- ISPs can take many forms as exemplified in the list of Austrian ASes: [4]
    - They can be large "classical" full range providers with (typically their own) land lines, mobile phone networks and other media, such as sub marine cables;
    - Purely mobile phone operators;[3]
    - Cable networks (which happens to be the largest provider in Austria in terms of IP addresses);
    - Private company networks; and
    - Municipal operators.

Nevertheless, they all have to, either by their own resources or in cooperation with other ISPs, operate the infrastructure of an autonomous system. This very infrastructure can be seen as a protected "asset" according to the Common Criteria for Information Technology Security Evaluation (CC) terminology. [5]

Result 1: Hence, an ISP, an instance of an AS with all the functionality associated with it, should be included in the NIS Directive in Annex II.

Furthermore, whether the NIS Directive makes use of the technical term "AS" or not is fundamentally a legalistic topic. In Recital 18 of the Directive, the term Autonomous System is defined as "a technically stand-alone network", which contrasts to the terminology of RFC 1930. It is recommended that RFC terminology be used in definitions in the NIS Directive.

3. The Internet Topology and its Physical Media

It is important to understand the basic layout of the internet because this influences the type of physical media and digital infrastructure that is used. The internet comprises of different types of ISPs that can be categorized into three tiers. Tier 1 providers, also called transit providers, are responsible for providing internet coverage over the entire internet region. These companies own or lease[4] from carriers terrestrial and sub marine fiber optic cables [6] that may expand thousands of kilometers all over the world and have a Settlement Free Peering relationship (SFP)[5] or transit free network, that is

[3] Which nevertheless operate their own land lines for connecting their masts.
[4] Fiber optical cable to be leased is called Dark Fiber. See https://www.luxconnect.lu/dark-fiber/, https://www.Hawe telekom.com/mapa-sieci
[5] As an example see the Settlement Free Peering agreements of TeliaSonera, Telxius and Deutsche Telekom. TeliaSonera https://web.archive.org/web/20160817032814/http://www.teliacarrier.com/dms/teliasoneraic/Documents/tsic-pp-10.pdf; Telxius, https://telxius.com/wp-content/uploads/2017/08/Peering-policy-Telxius.pdf; AT&T, https://www.corp.att.com/peering/; Deutsche Telekom, https://www.peeringdb.com/asn/3320

they do not pay to access their peer's network. Each ISP has connection points, Points of Presence (PoP), where service providers may connect,[6] at the end or along their physical lines.

The backbone of internet is a transit free network that enables Access Service Providers, known as Tier 2 providers, to connect to it for a payment, who in turn enable end-users to connect to the internet. Some Access Service Providers may have a SFP relationship with each other, if it is mutually beneficial but fundamentally, they pay to enable their internet traffic to pass through another internet service provider's network as shown in Figure 1. They too may own or lease physical media that enables the transmission of data, but on a much smaller scale than the Tier 1 ISPs. [7]

The final type of Internet Service provider is a Tier 3 ISP who pays for internet transit connecting to higher-tier ISPs, usually but not exclusively Tier 2 ISPs, in connecting the end customers to the internet. However, Tier 1 ISP may also have tier 3 ISPs or transit ISPs as their customers as well, who provide the so-called last mile Internet access and own or lease physical media to connect the end customer. They connect end customers to the internet via cable, DSL, fiber optic or wireless networks for example. The question arises, which parts ought to be protected by the NIS Directive.

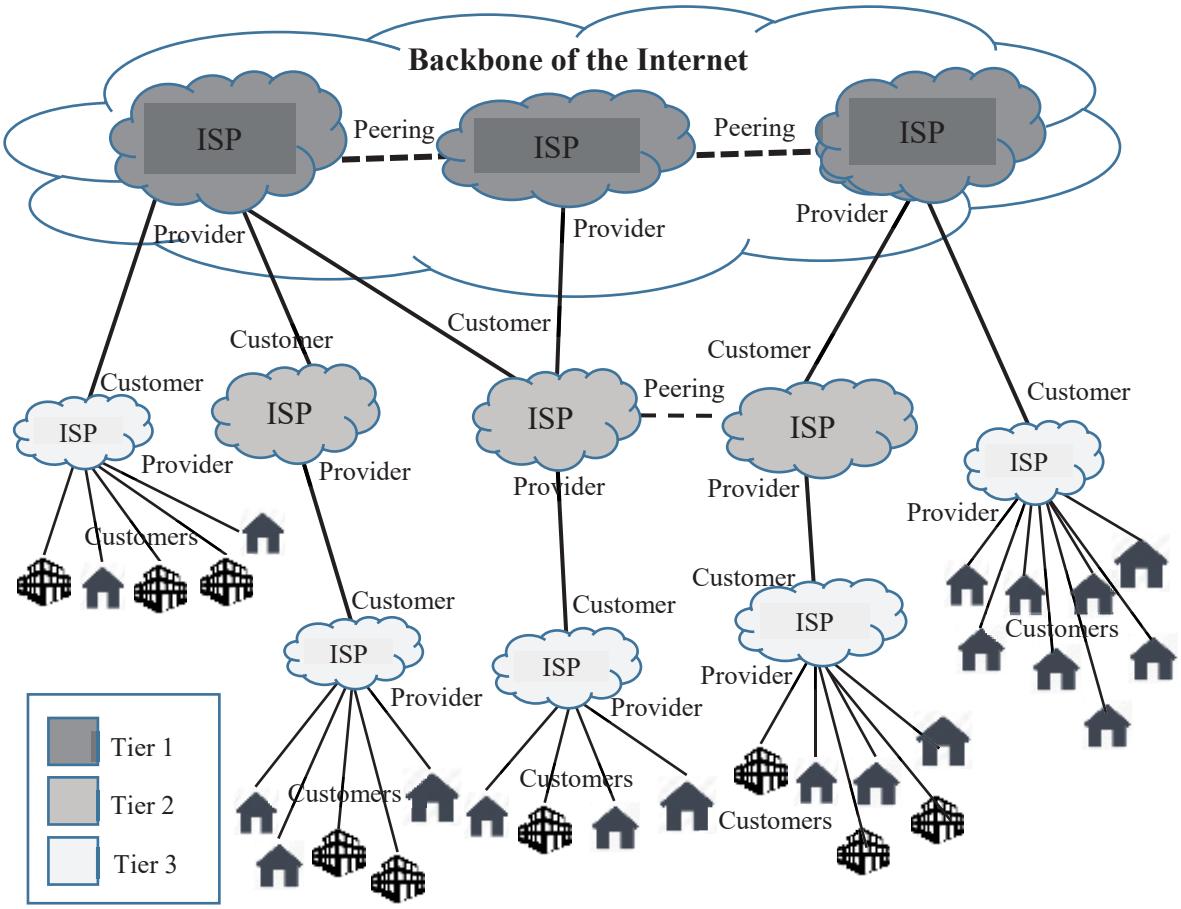

Figure 1: Internet Topology and ISP Tiers [7, p.116]

[6] Examples of PoP locations and fiber optic networks include Telia carrier's fiber optic network and PoP locations, https://www.teliacarrier.com/Our-Network.html, PoP locations of Deutsche Telekom Global Carrier, https://globalcarrier.telekom.com/network.

Physical media will vary according to the level of the ISP and their access to resource. The last mile service provider may use fiber optic, coaxial or twisted pair copper wire cabling, wireless or satellite links. The Tier 2 ISPs as shown predominantly make use of fiber optics, wireless or satellite links and the backbone itself predominantly uses fiber optic cable as it is the fastest and most efficient of all the transmission media widely used. Figure 2 is a summary of the transmission media. Furthermore, not all physical media is owned by the ISPs and hence they rely on the carriers to maintain them.

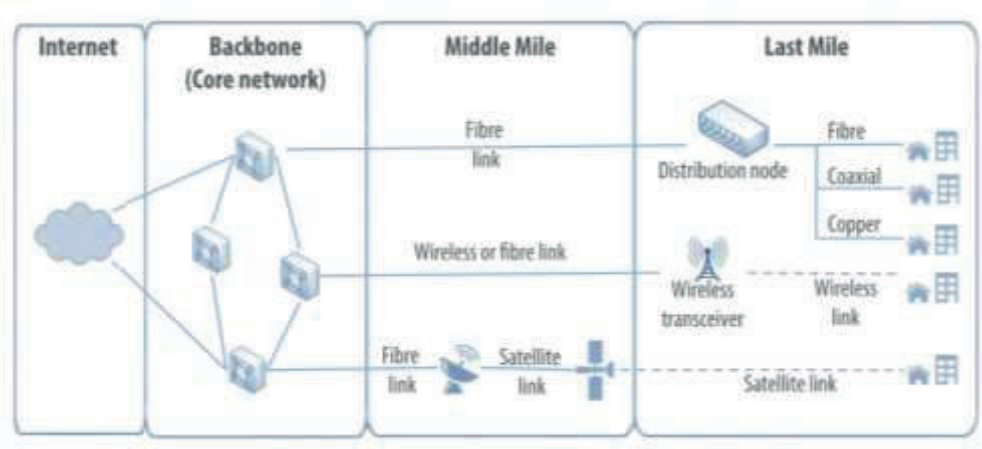

Figure 2: Segment from a Broadband Network [8]

Result 2: Tier 1-3 physical networks (including their access points) should be included in Annex II of the Directive.

4. How Autonomous Systems connect to each other

ISPs can connect to one another via private or public peering.

4.1. Private Peering

Private peering, also known as bilateral peering or Private Network Interconnect (PNI), is predominantly used by larger ISPs.[9] It is a direct connection into a data center or colocation center, usually using a simple dark-fiber cross-connect, between two peering routers.[10] Tier 1 ISPs make use of PNI because of the large amount of traffic between their peers. It also offers the most control due to the utilisation of the interface of traffic in both directions being clearly visible.[7, p. 127] This arrangement is most beneficial when there is large amounts of traffic and where ISPs want to choose with whom they share traffic to create a mutually beneficial exchange. Most PNI connections are located at carrier neutral colocation facilities and the costs are usually shared between the two ISPs peering (cf. the connection named “peering” in Fig. 1).

At this point, it is important to mention routers because they are fundamental in the functioning of the Internet. The routing process includes: (i) determining which links across a network should be used so that data is transmitted to the correct destination; (ii) transmitting data packets across the internetwork to its destination; and (iii) performing protocol conversions when the protocol used by connecting networks are different. [11, pp. 17f] Routing protocols are the software that enable the router to perform its function and the most common is Border Gateway Protocol (BGP). ISPs are essentially a network of routers and communication links. [3, 11] The responsibility of the routers is covered under the protection of ISPs because routers are an integral part of their infrastructure.

4.2. Public Peering

Public peering is done via an Internet eXchange Point (IXP)[7]. An IXP is defined as "*a physical network infrastructure operated by a single entity with the purpose to facilitate the exchange of Internet traffic between Autonomous Systems. The number of Autonomous Systems connected should at least be three and there must be a clear and open policy for others to join.*"[13] An IXP can also be seen as "*a layer 2 network where multiple network entities meet, for the purpose of interconnection and exchanging traffic with one another.*" [7, p.132]. An IXP usually began with a single layer 2 switch and as more participants connected, more switches were added. The European Internet Exchange Association (EURO-IX) states that an "*IXP is a single physical network infrastructure, (often an Ethernet local area network)*".[13] IXPs are popular because they enable smaller networks to connect together to provide Internet Service to a local area.

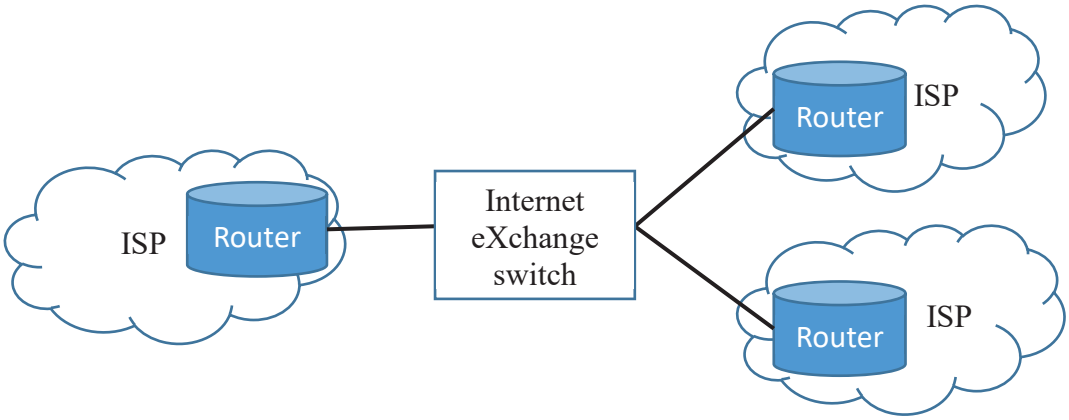

Figure 3: Internet eXchange Point (IXP)

Internet Service Providers can be commercially categorized into global, regional, national and local. IXPs facilitate that smaller ISPs join in order to cater for a particular area. They may enter into SFI agreements to provide transit to other participants and share the costs of connecting to a larger regional and/or global ISPs, which is usually costly. [14] It also facilitates the efficiency in routing Internet traffic and avoiding issues such as the trombone effect, where data takes a substantial detour to reach its destination. IXPs are essential in breaking the monopoly of larger ISPs and enable a more efficient and faster Internet Service in local and regional areas. Global ISPs may for example have PoP locations in major cities, such as London, Amsterdam, Sydney, Hamburg where it is most advantageous, which would leave many regional and local areas not covered. IXPs are essential in areas where it is difficult to lay terrestrial cables such as in densely populated cities or undeveloped countries who are looking to enable widespread Internet access in their country or area. [15] IXPs are usually managed by a separate entity, who is not an ISP and hence is not an ISP competitor in providing services to participants or end-users. [12] Therefore, IXPs are not necessarily the responsibility of the ISPs and therefore needs to be specifically addressed in the NIS Directive in order to protect this digital infrastructure.

Concerning the NIS Directive, there are 210 registered IXPs and 9,773 participants connected to IXPs in the European Union to date as shown in Table 1. Table 2 lists the top 3 IXPs with the most number of participants connected to IXPs in Europe. There are 807 participants connected to the Amsterdam

[7] Also called IX, exchange Point (EP), Internet Peering Point (IPP), Network Access Point (NAP) and Transit Exchange. [12]

Internet Exchange in the Netherlands for example, demonstrating the large number of ASes that are connected to just one Exchange Point.

EU Member States	No. IXPs	No. Participants	EU Member States	No. IXPs	No. Participants
Austria	6	204	Italy	12	649
Belgium	3	71	Latvia	3	42
Bulgaria	8	268	Lithuania	4	93
Croatia	1	34	Luxembourg	2	79
Cyprus	1	3	Malta	1	0
Czech Republic	5	315	Netherlands	14	1862
Denmark	5	106	Poland	13	1570
Estonia	4	38	Portugal	4	60
Finland	5	97	Romania	8	181
France	34	1124	Slovakia	3	108
Germany	35	1892	Slovenia	1	27
Greece	2	53	Spain	12	298
Hungary	1	67	Sweden	18	456
Ireland	5	76	**TOTAL**	**210**	**9773**

Table 1: Number of IXPs and participants per EU Member State
Collated by author from data at [16]

Country	City	Exchange Name	No. Participants
Netherlands	Amsterdam	Amsterdam Internet Exchange	807
Germany	Frankfurt	Deutscher Commercial Internet Exchange DE-CIX Frankfurt	776
Netherlands	Amsterdam	Neutral Internet Exchange	654

Table 2: The three largest IPXs in the European Union Member States
Collated by author from data at [16]

This data shows the massive scale of the infrastructure involved. There is, however, little information about the PNIs and the extent of their connections. IXPs are already in Annex II of the NIS Directive as critical infrastructure (see [2]).

The NIS directive states that an

"'*internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;*" [Article 4, (13)]

Firstly, the NIS Directive fails to protect PNI connections, connecting two ASes, which may be used to connect Tier 1 ISPs and many larger Tier 2 ISPs. Some IXPs have a small "service subnet" for monitoring and troubleshooting and may even host an email server and other services for members. Additionally the AS may provide routing information and information on network activity for its members such as a looking glass and commercial software is available and no doubt used to manage

IXPs.[8] It is common that an IXP be in itself an AS. The NIS Directive's definition would exclude these IXPs and hence they are not protected.

Result 3: The author recommends that the NIS Directive include and hence protect all points of exchange from the very basic such as a port-to-port connection right through to commercially managed IXPs, which are in themselves Autonomous Systems managed by commercial software.

5. Registries and their implementation on the Internet

The NIS Directive in Annex II, lists Top Level Domain (TLD) name registers as critical infrastructure[9] and hence it is the author's proposal that two registries that are closely related to TLD and fundamental to the internet should also be included, namely AS and IP registries.

5.1. AS and IP registers

The Internet Assigned Numbers Authority (IANA), located in the US, is responsible for globally coordinating the "*full range of IPv4 and IPv6 addresses and the whole 32-bit Autonomous System (AS) Number range* and ensuring the uniqueness of the full set of these Internet resources. [16, 17] IANA allocates AS numbers and IP address blocks to five Regional Internet Registries (RIRs), namely APNIC (South/East Asia, Oceania), ARIN (US, Canada), RIPE NCC (Europe, Central Asia, Arabia), LACNIC (Latin America), and AFRINIC (Africa). [10]

An IP address is a unique identifier that enables the navigation of data packets to a recipient on the Internet. Furthermore, information is stored pertaining to IP addresses such as: (i) postal address of registrant, (ii) location of the user; (iii) routing information; (iv) services such as email, DNS, HTTP; (v) History; and (vi) Abuse. [18] The ability to be able to match up a person or entity and location with an IP address goes a long way combatting cyberattacks. There are two types of Internet Protocols, namely, (i) IPv4, which is a 32-bit address space, which creates an address pool of 2^{32} in size; and (ii) IPv6, 128-bit address space, which is 2^{128} in size. [19] On the 3rd of February 2011, IANA declared that the IPv4 central address pool was depleted, after having allocated the last of its IPv4 addresses. IPv4 contained over 4.3 billion IP addresses. The solution was to introduce the Internet Protocol IPv6 [20], which created an additional 340 x 10^{36} IP addresses, which was successfully deployed. IANA allocates RIRs IPv6 address space when a RIR's IPv6 addresses are: (i) less than 50% of a /12; or (ii) less than its established necessary space for the following 9 months. In every case, IANA makes a single allocation to satisfy a RIR's established necessary space for 18 months [21].

An Autonomous System Number (ASN) uniquely identifies a group of IP networks run by one or more network operators with a single clearly defined routing policy. Information that is required for an applicant to receive an ASN is the applicants peering partners ASNs (at least two), their contact details and the routing policy in the Routing Policy Specification Language [22]. Each registry has a pool of AS Numbers (ASNs) from IANA and when this pool reaches a low threshold of either 20%

[8] European Internet Exchange Association (Euro-IX), https://www.euro-ix.net/en/forixps/set-ixp/ixp-bcops/technical-recommendations/ixp-management/
[9] NIS Directive, Annex II
[10] https://www.apnic.net/about-apnic/organization/history-of-apnic/history-of-the-regional-internet-registries/, https://www.icann.org/en/system/files/files/what-icann-does-22jun12-en.pdf, https://www.ripe.net/manage-ips-and-asns/db/support/documentation/ripe-database-documentation/download-as-a-pdf

or the number of free ASNs is less than its two month need, IANA allocates another 1024 block of AS numbers.[11]

RIPE NCC, "Reseaux IP Europeens" Network Coordination Center is responsible for Europe, the Middle East, and Central Asia's Regional online Internet Registry and the EU Member States lie within its domain. Members of RIPE NCC called Local Internet Registries (LIRs) receive blocks of IP addresses and AS numbers, allocated by RIPE NCC, who in turn distribute them to end users. According to RIPE NCC, LIRs are ISPs, academic institutions, telecommunication companies and large enterprises[12] and LIRs must be a legal entity in the RIPE NCC service region.[13] There are 25,353 LIRs in the RIPE NCC region to the date of this publication.[14] The RIPE NCC database, according to the RIPE Database Documentation manual contains allocations and assignments of IP address space, reverse domain registrations, routing policy information (Internet Routing Registry (IRR)), contact information for the Internet resources used in the operation of networks or routers, and their organisations.[15] The IRR contains the routing policy of operators and their BGP route origins.[16] It is used to assist in debugging, configuring and engineering routing and addressing. The IRR enables the mapping of an origin AS to a list of networks and the validating of BGP announcement messages.[17] In relation to the database an "*AS is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy*", where the word prefix refers to "*one or more networks*".[18]

Result 4: Therefore, in order for the Internet to function it requires both ASes and the IP address space registers to remain up to date and complete. Hence, the registries, which are in the EU Member States region, administered by RIPE NCC, should be included in the NIS Directive in Annex II as critical infrastructure.

5.2. Top Level Domain (TLD) Registries

A TLD register contains all the top-level domains. The TLD name is the last part of the domain name that follows the last dot. For example, www.google.com, the TLD is .com. The generic TLDs, called gTLDs, initially published in the 1980s were .COM, .EDU, .GOV, .INT, .MIL, .ORG and .NET. [19]

As of April 2020, there are 1513 TLDs[20] and this number is expanding yearly. The TLD name list is managed by Internet Corporation for Assigned Names and Numbers (ICANN) based in the United

[11] See section on RIR Pools, https://www.potaroo.net/tools/asn16/, https://www.icann.org/resources/pages/global-policy-asn-blocks-2008-07-31-en; For the ASNs assigned to the RIRs, see https://www.iana.org/assignments/as-numbers/as-numbers.xhtml#as-numbers-2; For the IPv4 address space assigned to the RIRs, see https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml; For the IPv6 address space assigned to the RIRs, see https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml

[12] https://www.ripe.net/participate/member-support/payment/russia/RussianFactBookEN.pdf, For a list of LIR in each country in the RIPE NCC's domain, https://www.ripe.net/participate/member-support/list-of-members/europe

[13] https://www.ripe.net/about-us/what-we-do/ripe-ncc-service-region

[14] https://labs.ripe.net/statistics/number-of-lirs

[15] https://www.ripe.net/manage-ips-and-asns/db/support/documentation/ripe-database-documentation/download-as-a-pdf, p. 11.

[16] https://www.ripe.net/manage-ips-and-asns/db/support/managing-route-objects-in-the-irr

[17] http://www.irr.net/docs/overview.html

[18] ftp://ftp.ripe.net/ripe/docs/ripe-234.txt

[19] http://archive.icann.org/en/tlds/

[20] http://stats.research.icann.org/dns/tld_report/, For a current list of all of TLDs registered with IANA, https://data.iana.org/TLD/tlds-alpha-by-domain.txt

States with a regional office in Belgium.[21] Among other functions, ICANN is responsible for "*the generic (gTLD) and country code (ccTLD) Top level Domain Name System management and root server system management functions*."[22] The DNS translates a domain name typed into a web browser into an IP address and connects the user to the desired website.[23] The TLDs are transferred and stored in root Domain Name Systems (DNS), also referred to as the "*the phone book of the Internet*" [23], situated around the world connected to the Internet. ICANN is also an operator of the root DNS, l.root-servers.net. ICANN delegates the responsibility for registering gTLDs to its affiliates, only registering domain names for .INT.

There are over 2000 accredited ICANN registrars or resellers,[24] who are accredited by ICAAN and certified by the registries to sell gTLDs.[25] ICANN registrars are bound by a Registrar Accreditation Agreement and are required to register gTLDs by submitting data to registry operators,[26] who are responsible for generating the zone files for the root DNSs.[27] Mirrored root DNS servers are located around the world, including in Europe as shown in Figure 4.

5.3. Root Domain Name System (DNS)

A DNS is responsible for resolving unique alphanumeric domain names with IP addresses. [24] Using Domain Names makes it easier for users to remember and if the physical location moves, then Domain Name can be easily changed to reflect the new location that is the new IP address. [25] As of the 16th of April, 2020, there were 1088 instances of 13 Doman Name Root Servers situated across the world operated by 12 organisations, who are responsible for their upkeep. Table 3 lists the operators, the Domain Name root server or host name, its IP address and the total number of duplicated server sites for which the operators are responsible.[28] One of them is directly relevant to the EU, depicted in bold.

Host Name	IP address	No. Sites	Operators
a.root-servers.net	IPv4: 198.41.0.4 IPv6: 2001:503:ba3e::2:30	53	VeriSign, Inc.
b.root-servers.net	IPv4: 199.9.14.201 IPv6: 2001:500:200::b	6	Information Sciences Institute
c.root-servers.net	IPv4: 192.33.4.12 IPv6: 2001:500:2::C	10	Cogent Communications
d.root-servers.net	IPv4: 199.7.91.13 IPv6: 2001:500:2D::D	156	University of Maryland
e.root-servers.net	IPv4: 192.203.230.10 IPv6: 2001:500:a8::e	308	NASA Ames Research Center
f.root-servers.net	IPv4: 192.5.5.241 IPv6: 2001:500:2f::f	252	Internet Systems Consortium, Inc.
g.root-servers.net	IPv4: 192.112.36.4 IPv6: 2001:500:12::d0d	6	Defense Information Systems Agency
h.root-servers.net	IPv4: 198.97.190.53 IPv6: 2001:500:1::53	8	US Army (Research Lab)

[21] https://newgtlds.icann.org/en/about/program; https://forms.icann.org/en/contact
[22] https://www.icann.org/resources/pages/cctlds-21-2012-02-25-en
[23] https://www.icann.org/resources/pages/cctlds-21-2012-02-25-en
[24] https://www.icann.org/registrar-reports/accreditation-qualified-list.html
[25] https://www.icann.org/resources/pages/register-domain-name-2017-06-20-en
[26] https://www.icann.org/en/system/files/files/approved-with-specs-27jun13-en.pdf
[27] https://www.domaintools.com/support/what-is-icann-and-how-is-it-related-to-registries-and-registrars#
[28] https://root-servers.org/

i.root-servers.net	IPv4: 192.36.148.17 IPv6: 2001:7fe::53	70	Netnod
j.root-servers.net	IPv4: 192.58.128.30 IPv6: 2001:503:c27::2:30	185	VeriSign, Inc.
k.root-servers.net	**IPv4: 193.0.14.129** **IPv6: 2001:7fd::1**	**76**	**RIPE NCC**
l.root-servers.net	IPv4: 199.7.83.42 IPv6: 2001:500:9f::42	165	ICANN
m.root-servers.net	IPv4: 202.12.27.33 IPv6: 2001:dc3::35	9	WIDE Project

Table 3: Domain name route servers and their operators
Author's collation, source https://root-servers.org/

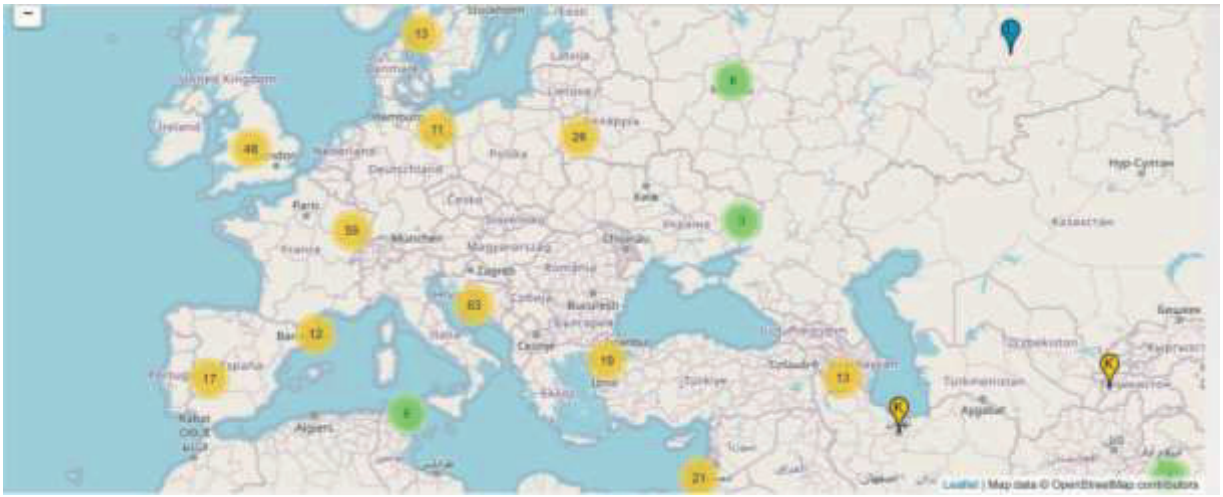

Figure 4: Root DNSs in Europe
Source https://root-servers.org/

The DNS is a critical part of the Internet because nearly all services need the ability to resolve names and addresses in the globally unique DNS namespace,[29] and therefore the root DNS providers should be included in the NIS Directive in Annex II as providers of critical infrastructure. The difficulty with this is that the operators or service providers, as stated in Annex II of the NIS directive, are not all located in EU Member States, even though (mirrored) root Domain Name Servers themselves are. It may make sense to name the digital critical infrastructure opposed to the entities that are responsible for them in the NIS Directive.

Result 5: The TLD registries and the DNS service providers are included in Annex II as critical infrastructure, however DNS service providers should be changed to root DNS Service providers, because the root DNS servers are not protected under the term ISP.[30]

6. Conclusion

The most pressing addition to the critical infrastructure that the author is proposing to be included in the NIS Directive, particularly but not exclusively in Annex II, is Internet Service Providers (ISPs) as they are the essential operators, quasi the building blocks of the Internet, which enable among other

[29] Threat Mitigation for the Root Server System, https://root-servers.org/publications/Threat_Mitigation_For_the_Root_Server_System.pdf
[30] The current NIS Directive fails to account for the difference between DNS infrastructure that is part of an AS and DNS servers outside the "administration" (see RFC 1930) of an AS (a.k.a. ISP).

things end users to connect to the Internet. The NIS Directive includes the TLD registry but failed to recognise that it has dependents particularly information in registries such as the IP address space registry for IP addresses are unique identifiers of every connection on the Internet and hence is fundamental to its functioning. Furthermore, AS registries should also be included as critical infrastructure as they define every network on the Internet and enable data packets to be routed to their destinations and without this numbering system, data would never be able to find its way in the vastness of the Internet. In this way, it is a given that the DNS be included in the NIS Directive, however, this should be read root DNS as every network on the Internet can have its own DNS server. The truly critical infrastructure and that infrastructure that is not under the jurisdiction of ISPs is the root Domain Name System.

7. References

[1] Directive (EU) 2016/1148, http://data.europa.eu/eli/dir/2016/1148/oj

[2] BAGNATO, D., The NIS Directive and the Smart City, Transylvanian eGovernment Conference, Cluj, Romania, 2019, forthcoming.

[3] RFC 1930, https://tools.ietf.org/html/rfc1930#section-3

[4] https://ipinfo.io/countries/at

[5] Common Criteria for Information Technology Security Evaluation (CC), Part 1, https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[6] Map of underwater internet cables, https://www.submarinecablemap.com/

[7] ERGUN, O., Service Provider Networks, OE Publishing, Istanbul, 2019

[8] European Court of Auditors, Broadband in the EU Member States: despite progress, not all the Europe 2020 targets will be met, 2018, https://www.eca.europa.eu/Lists/ECADocuments/SR18_12/SR_BROADBAND_EN.pdf

[9] Packet Clearing House, Internet Exchange Directory, Statistics, https://www.pch.net/ixp/dir

[10] Federal Communications Commission, FCC Record: A Comprehensive Compilation of Decisions, Reports, Public Notices, and Other Documents of the Federal Communications Commission of the United States, Volume 16, Item 73-75

[11] BHARADWAJ, P., Routers in Internetworks: How Data travels through the Internet, https://link.springer.com/content/pdf/10.1007/BF02902525.pdf

[12] JENSEN, M., Promoting the Use of Internet Exchange Points: A Guide to Policy, Management, and Technical Issues, Internet Society Reports, 2012(02) https://www.internetsociety.org/wp-content/uploads/2012/12/promote-ixp-guide.pdf

[13] European Internet Exchange Association, What is an IXP, https://www.euro-ix.net/en/forixps/

[14] RFC 1132, A Standard for the Transmission of 802.2 Packets over IPX Networks, https://tools.ietf.org/html/rfc1132

[15] Packet Clearing House, Internet Exchange Directory, https://www.pch.net/ixp/dir

[16] SNYDER, J., KOMAITIS, K., ROBACHEVSKY, A., The History of IANA: An Extended Timeline with Citations and Commentary, Internet Society, 2017, https://www.internetsociety.org/wp-content/uploads/2016/05/IANA_Timeline_20170117.pdf

[17] RIPE Network Coordination Center, Management Process for IPs and ASNs, https://www.ripe.net/manage-ips-and-asns/db/support/documentation/ripe-database-documentation/download-as-a-pdf

[18] GUÐMUNDSSON, O., What do we know about an IP address? RIPE Labs, https://labs.ripe.net/Members/olafur_gudmundsson/what-do-we-know-about-an-ip-address?pk_vid=f21819e2d62bb2f51587344761335273

[19] Internet Assigned Numbers Authority, https://www.iana.org/numbers

[20] RIPE Network Coordination Centre, IP addressing, https://www.ripe.net/about-us/press-centre/understanding-ip-addressing

[21] ICANN Archives, https://archive.icann.org/en/policies/proposed-ipv6-policy-14jul06.htm

[22] RIPE Network Coordination Center, Supporting Notes for Internet Address Space Request Forms, https://www.ripe.net/manage-ips-and-asns/resource-management/supporting-notes-for-internet-address-space-request-forms#ASN

[23] ICANN, What ICANN does and doesn’t do, https://www.icann.org/en/system/files/files/what-icann-does-22jun12-en.pdf

[24] WANDER. M., BOELMANN, C., and WEIS, T., Domain Name System Without Root Servers, https://link.springer.com/content/pdf/10.1007%2F978-3-319-76687-4_14.pdf

[25] PARE, D. J., Internet Governance in Transition, Who is the Master of this Domain, 2002, p. 10

All web sources as per March 31, 2020