Internet Impact Brief

Revised Directive on Security of Network and Information (NIS2) – Presidency Compromise Proposal September 2021

Callum Voge, Internet Society
Olaf Kolkman, Internet Society
Andrei Robachevsky, Internet Society

Version 1.1 (8 November 2021)

Abstract

In December 2020, the European Commission proposed the Revised Directive on Security of Network and Information (NIS2), repealing the existing cybersecurity rules. This new proposal may have implications for key Internet infrastructure providers including Domain Name System services, Top-Level Domain registries, trust service providers, and certificate authorities that operate in the European market. This report uses the Internet Impact Assessment Toolkit[1] (IIAT) to assess how the Presidency compromise proposal[2] from 21 September 2021 may affect the global Internet by impacting what the Internet needs to thrive as an open, globally connected, secure and trustworthy resource for all.

Context and Assumptions

Introduction: the Revised Directive on Security of Network and Information

The Revised Directive on Security of Network and Information[3], commonly referred to as NIS2, was proposed by the European Commission on 16 December 2020. The revised directive introduces

Methodology

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). This includes: an accessible Infrastructure with a common protocol, a layered architecture of interoperable building blocks, decentralized management and distributed routing, a common global identifier system, and a technology neutral, general-purpose network.

To assess whether the present proposal has an impact on the Internet, this report will examine its impact on the IWN foundation the Internet needs to exist, and what it needs to thrive as an open, globally-connected, secure and trustworthy resource.

[1] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/ The IIAT was developed by the Internet Society[1] to be used by anyone who wants to check if a particular policy, development, or trend affects the critical properties of the Internet Way of Networking (IWN), and Enablers of an Open, Globally-Connected, Secure and Trustworthy Internet.

[2] 12019/21

[3] https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

new cybersecurity rules for the EU and will replace the existing 2016 Network and Information Systems (NIS1).[4]

The NIS2 proposal seeks to respond to the rapidly changing cybersecurity threat landscape as well as the limitations of the existing NIS1. The proposal's objective is to support a more resilient Europe by protecting additional vulnerable sectors and increasing interconnectivity between Member States' cybersecurity mechanisms. Accordingly, Member States will need to transpose the Directive into national laws.

The NIS2 proposal differs from the NIS1 in a number of ways. The directive's scope has been expanded under NIS2 to cover additional sectors including telecoms, social media platforms, and public administration.[5] The NIS2 proposal also removes the distinction between Operators of Essential Services (OES) and Digital Service Providers (DSP) found in the NIS1.[6] Instead, Member States will enforce risk management and reporting requirements for "essential and important entities," with digital infrastructure designated as "essential" and digital providers as "important entities."[7]

The concrete list of entities that will fall under NIS2 will be created by Member States while the Directive itself defines a high-level list of entities in the Annex. In this analysis we will focus on a subset of these entities, primarily concerned with Domain Name System (DNS) and trust services providers.

A) *DNS Services within the Scope of NIS2 Requirements*

The Domain Name System (DNS) plays a crucial role in making the Internet easier to navigate, using a system of common global identifiers that systems and users worldwide can depend on to get them where they are trying to go on the Internet. DNS services do this by creating a semantic map that allows users to navigate the network using only domain names (e.g. internetsociety.org) rather than requiring users to remember multiple numerical network addresses (e.g. 104.18.16.166 or 2606:4700::6812:11a6). The links created by DNS services ensure consistency and help prevent the fragmentation of the Internet.

The 21 September NIS2 compromise proposal holds all providers of DNS services along the DNS resolution chain within scope, including: (1) operators of root name servers; (2) top-level-domain (TLD) name servers; and (3) authoritative name servers for domain names and recursive resolvers.[8]

[4] https://digital-strategy.ec.europa.eu/en/policies/nis-directive

[5] https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2

[6] https://www.cullen-international.com/news/2021/04/NIS2--Overview-of-the-new-EU-cybersecurity-rules-proposed.html

[7] https://www.digitaleurope.org/resources/digitaleuropes-position-on-the-nis-2-directive/

[8] Recital 15, 12019/21.

"Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the

NIS2 requires that DNS services within the proposal's scope meet certain reporting and security policy requirements, with exceptions for small and micro entities.[9] These requirements include incident reporting, the designation of a representative if the entity is located outside of the Union, and the adoption of various supply chain security measures. Given the typical size of DNS services, very few entities would qualify for exemptions under the category of small and micro entities.

B) Top Level Domain Registries within the Scope of NIS2 Requirements

Top Level Domains (TLDs) sit near the top of the DNS and can be identified by the last segment of a domain name (e.g. .com, .org, .net, or .uk). A TLD registry is a database of all the domain names registered under one of these TLDs.

Operators of TLD registries are responsible for the registration of domain names either directly (as a registry) or through a network of domain name resellers (registrars). TLD registry operators primarily manage the generation, signing, and publication of the technical information needed for delegation to the next level in the DNS name hierarchy.

When zone data is out of date or inaccurate, the links connecting the TLD to its underlying consumer domain names break, causing traffic to be directed to inaccurate or outdated network addresses. This creates security risks as users are taken to insecure network addresses where they can become victim to abusive behavior. Weak registration policies make abuse of the DNS even easier, as evidenced by instances of domain names being used as botnet command and control centers for attacks.

The NIS2 proposal places requirements on TLD registries to collect domain name registration data by implementing technical and organizational measures.[10] Additionally, TLD registries will have 72 hours to

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." [SIC]

[9] Article 2(2). 12019/21.
"Regardless of the size of the entities referred to in paragraph 1, this Directive also applies to entities referred to in the Annex, where: (a) the services are provided by one of the following entities: (iv) top–level domain name registries ~~and domain name system (DNS)~~ referred to in point 8 of the Annex" [SIC]

[10] Recitals 59-64, 12019/21.

reply to requests from legitimate access seekers for the disclosure of domain name registration data.[11] There are no exceptions in the NIS2 proposal for small or micro trust service providers.[12]

C) Trust Service Providers within the Scope of NIS2 Requirements

Trust service providers (TSP) provide and maintain digital certificates that are used to create and validate electronic signatures as well as to authenticate signatories and websites. They play a critical role in verifying the identity of people and companies on the Internet. The reliable use of digital certificates increases the trustworthiness of the Internet and has enabled, among other things, the growth of eGovernment services, as well as sensitive health and financial services, throughout the EU.

The most recent compromise proposal of NIS2 includes TSPs within the scope of the Directive[13] and identifies them as essential entities in the Annex under the category of digital infrastructure.[14] As essential entities, TSPs would be subject to both ex-ante and ex-post supervision[15], meaning that trust service providers would need to systematically document their compliance with the security requirements of the directive. There are no exceptions in NIS2 for small or micro trust service providers.[16]

How does NIS2 Affect the Internet?

In order to understand how NIS2 affects the Internet itself we assess how it might impact the Critical Properties of the Internet Way of Networking as described by the Internet Society[17].

[11] Recital 48. 12019/21.

[12] Article 2(2). 12019/21.
"Regardless of the size of the entities referred to in paragraph 1, this Directive also applies to entities referred to in the Annex, where: (a) the services are provided by one of the following entities: (iv) top–level domain name registries ~~and domain name system (DNS)~~ referred to in point 8 of the Annex" [SIC]

[13] Recital 48. 12019/21.

[14] Annex. Item 8, Digital Infrastructure. 12019/21.

[15] https://www.cullen-international.com/news/2021/04/NIS2–Overview-of-the-new-EU-cybersecurity-rules-proposed.html

[16] Article 2(2). 12019/21.
"Regardless of the size of the entities referred to in paragraph 1, this Directive also applies to entities referred to in the Annex, where: (a) the services are provided by one of the following entities: (ii) qualified trust service providers referred to in point XX of the Annex; (iii) non-qualified trust service providers referred to in point XX of the Annex;" [SIC]

[17] https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

Interoperable and reusable building blocks that are openly defined and voluntarily adopted by a user community.

A key feature of an open Internet is that it facilitates fast and permissionless innovation so that useful changes are adopted when needed and unnecessary ones removed without barriers. The NIS2 proposal has been successful in not prescribing specific security mechanisms to DNS services and has instead taken a technology neutral approach.

Technological flexibility has proved important in the past as DNS services have adopted new security building blocks such as Domain Name System Security Extensions (DNSSEC) as well as DoT and DoH to respond to new challenges. In this sense, whileNIS2 does confine DNS services in developing their own measures appropriate to their risk level, it is positive that the type of technologies used to meet these requirements has largely been left open.

Decentralized Management and a Single Distributed Routing System which is scalable and agile

The decentralized management of Internet services allows for local optimization as needed. The NIS2 proposal places new obligations on DNS services without considering the wide variety of existing obligations they already face under a myriad of community-led governance structures. This approach risks the creation of multiple layers of accountability and clashing obligations, threatening the autonomy of DNS services and resilience of the Internet. For example, the requirements for certain country code top-level domains are set by local government while others are set by local communities. Adding regulations at higher levels would negate local community-led governance structures and reduce autonomy.

Common Global Identifiers which are unambiguous and universal

The globally connected Internet uses common identifiers to deliver consistent addressability and prevent Internet fragmentation. By placing additional requirements on DNS services, without consideration for differences in resources and ability, NIS2 disproportionately burdens certain entities. Entities that fail to comply with obligations may be ordered by member states to "cease non-compliant conduct".[18] Could failure to comply result in banning certain domain names in the EU and barring access for EU residents? By not providing greater clarity on repercussions, NIS2 creates the conditions for the

[18] Article 29(4). 12019/21.
"Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power at least to: (c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct" [SIC]

disintegration of common global identifiers and contributes to Internet fragmentation.

Fragmentation may also occur when global entities within the scope of the directive change their behavior to avoid administrative fines. Global entities could do this by ceasing to provide their services to European Internet users – geo-blocking European DNS queries and likewise contributing to Internet fragmentation. Historic examples of regulation-dodging behaviour can be seen in General Data Protection Regulation (GDPR) cases where websites based outside the EU blocked access from Europe.[19]

Furthermore, new obligations on TLDs could interfere with global governance rules resulting in Internet fragmentation. The equivalent treatment of all TLD registries under the NIS2 proposal causes problems when applied to country code top-level domains (ccTLDs). Would ccTLDs associated with non-EU countries (such as .us, .uk, or .cn) be in scope if they include lower-level domain names from EU registrants or are used by the websites providing services in the EU? Similarly, what about generic ccTLDs such as .tv that are used across national borders? The broad treatment of all TLD registries creates issues of extraterritoriality and could further encourage Internet fragmentation if regulatory actions also come from other countries.

The compromise proposal retains within its scope both root name servers as well as the Address and Routing Parameter Area (.arpa) TLD, with the operators of root name servers identified explicitly. Root name servers sit at the core of the DNS—like the foundation a tree trunk serves for branches and leaves – and answer requests for records in the root zone, which contains the list of root servers themselves as well as a list of the authoritative name servers for all TLDs.

Meanwhile, .arpa provides a number of critical technical services for the global Internet[20] including a "reverse resolution service" where numerical IP addresses are translated into their corresponding domain names. The service provided by .arpa as a TLD is essential to the functioning of global common protocols. It is currently governed by the Internet Architecture Board, a multi-stakeholder committee associated with the Internet Engineering Taskforce (IETF), the standards body for the Internet.

NIS2 imposes a top-down Internet governance approach for root name servers and .arpa which could fuel Internet fragmentation, especially if similar top-down approaches were to be implemented by other governments around the world. This would harm multistakeholder processes and contribute to

[19] https://www.bbc.com/news/technology-44614885

[20] Services offered by .ARPA are documented in RFC1035 (in-addr.arpa),), RFC3152 (ip6.arpa), RFC3404 (uri.arpa & urn.arpa), RFC4698 (iris.arpa), RFC5855 (in-addr.servers.arpa and ip6-servers.arpa), e163.arpa (RFC6166), RFC7050 (ipv4only.arpa), and RFC 7535 (as112.arpa)

the disintegration of common global identifiers. Furthermore, it runs contrary to the EU's historic support of a "single, open, neutral, free, secure and un-fragmented network". The NIS2 proposal should therefore exclude root name servers and the .arpa TLD from the directive.

Summary

NIS2 affects three critical properties that underpin the Internet predominately due to the wide variety of DNS services that fall under the current scope. Various DNS services participate in different community-led governance efforts that may be in conflict with the requirements of NIS2. This could have consequences for permissionless innovation on the Internet, Internet resilience, and Internet fragmentation.

How does NIS2 Affect the Realization of the Full Potential of the Internet?

The critical properties are what is needed to have the Internet, but they are not sufficient if we want the Internet to reach its full potential. The Internet Society advocates for an Internet that is Open, Globally Connected, Secure and Trustworthy – strongly aligned with the EU vision of a "single, open, neutral, free, secure and un-fragmented network". In order to assess how we get to an Internet with these characteristics, we will look at these through the lens of the enablers of these goals[21].

Collaborative development, management, and governance

The Internet's technologies and standards are developed, managed, and governed in an open and collaborative way. This open collaboration extends to the building and operation of the Internet and services built on top of the Internet. The development and maintenance process is based on transparency and consensus, and has as its goal the optimization of infrastructure and services to the benefit of the users of these technologies.

Internet security problems are global in nature and therefore require global coordination, which is best accomplished through voluntary collaboration, not regulation. This change undermines consensus-based decision making and constrains efforts to ensure that infrastructure and services are optimized for the benefits of users.

By not recognising the wide variety of structures that govern DNS services, the NIS2 proposal risks replacing existing collaborative multistakeholder development with a top-down approach that would

[21] https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

only achieve a narrow subset of global needs.

Unrestricted reachability

Unrestricted reachability means that Internet users have access to all the resources and technologies made available on the Internet and are able to make resources available themselves. Once a resource has been made available in some way by its owner, there is no blocking of legitimate use and access to that resource by third parties.

NIS2 creates a number of challenges for global DNS services that may struggle to comply with the proposal. Internet domain registrars such as GoDaddy may need to stop registering domains from EU citizens in non-compliant TLDs. Similarly, TLD authoritative servers may need to stop answering queries from EU resolvers, even though many of these queries are proxied by public DNS resolvers run by Google, Cloudflare, and others at the request of EU businesses and Internet users. Other enforcement mechanisms may involve mandated filtering at the resolver level, which would similarly restrict reachability to unwitting third parties, namely the registrars of the associated TLD. These scenarios would deprive EU Internet users of the essential systems and resources generated by DNS services. Over time, the Internet experienced by European users would appear vastly different to that enjoyed by the outside world, cutting Europeans off from new knowledge and innovation driven by the Internet.

Similarly, NIS2 may require non-compliant Certificate Authorities (CAs)[22] to be removed from the set of trusted CAs in browsers. This could lead to EU-specific versions of popular browsers like Chrome and Safari. Non-compliant CAs may likewise find that access to the web resources protected by their certificates is denied or becomes insecure. This would deprive EU residents from access to parts of the Internet.

Even if TLDs were to operate exclusively in the EU, issues of reachability would still arise. The NIS2 proposal empowers member states to 'cease non-compliant action', which could result in the barring of TLDs from registering names until they are able to collect all mandatory registration information. This would similarly deny Internet users the full benefits of DNS services.

[22] Certificate Authorities (CAs) are a critical component of Public Key Infrastructure (PKI), which is a system of creating, managing, and using digital keys and certificates. CAs issue digital certificates that certify the ownership and authenticity of a public encryption key., ensuring that the public key offered by a website does indeed belong to the website. CAs therefore ensure the authenticity, integrity, and confidentiality of communication on the Internet. Without CAs, third parties could impersonate other communicating parties to eavesdrop or tamper in message exchanges. These vulnerabilities could additionally be used to spread malware or imitate banks and other sites to steal users' credentials

Finally, a similar issue may arise for technologies and resources provided by third parties along the supply chain, which typically conduct their own security analyses and are evaluated for safety by consumers of their services. NIS2 could result in the barring of these services in the EU while administrative fees could result in bankruptcy for smaller players and market consolidation by larger players. These trends would limit the diversity of services on the Internet, to the determent of European Internet users.

Integrity of information, applications, and services

The value of the Internet is maximized when the integrity of data sent over the Internet, and stored in applications, is not compromised. This protection means that critical underlying Internet services, such as DNS and the routing system, cannot be manipulated or compromised by malicious actors.

NIS2 is commendable for recognizing the importance of integrity and encouraging the use of important tools like encryption. Yet while the use of tools like encryption should be pursued by European entities, other well-intentioned obligations under NIS2 may have unintended negative consequences for the integrity of data if they are too stringent and cannot be followed. For example, Certificate Authorities (CAs) that fail to meet obligations under NIS2 may be removed from the set of trusted CAs in browsers, even if they adhere to the trust criteria mutually agreed among certificate authorities, browser manufacturers, and other relevant stakeholders. This would negatively affect access to the services protected by the certificates that these CAs issue, creating opportunities for man-in-the-middle attacks, impersonation of services, and other malicious actions.

The NIS2 proposal has a further opportunity to strengthen Internet security so that the integrity of data sent through the system is not compromised. Networks constantly exchange routing information to get Internet traffic to where it needs to be. Hundreds of incidents occur on these networks everyday including route hijacking, route leaks, and IP address spoofing. These incidents result in Denial of Service (DoS) attacks, surveillance, and lost revenue, negatively impacting the trustworthiness of the Internet.

Voluntary collaborative actions are essential for countering incidents such as these and increasing Internet security. For example, the Internet Society coordinates and supports an industry-led initiative called the Mutually Agreed Norms for Routing Security (MANRS) to protect the integrity and resilience of the Internet. The initiative supports four voluntary programs for network operators (ISPs), Internet exchange points (IXPs), content delivery networks (CDNs) and cloud providers, and equipment vendors to implement practices to combat the most common routing threats. We recommend that NIS2 encourage voluntary collaborative actions that increase Internet security.

Reliability, resilience, and availability

The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service's availability is unpredictable, then users will observe this as unreliable. This can reduce trust not just in one single service, but in the Internet itself. Resilience is related to reliability: a resilient Internet maintains an acceptable level of service even in the face of errors, malicious behavior, and other challenges to its normal operations.

Digital service providers may find their resources strained when complying with NIS2 requirements alongside existing obligations developed through community-led governance efforts. This could fuel market exit, business closures, or the acquisition of smaller entities by larger entities, resulting in market concentration. Market consolidation of DNS services would reduce choice and resilience on the Internet. When the number of providers is limited, errors, malicious behaviour, or other challenges to normal operations are no longer isolated and shock the entire system.

Non-profit certificate authorities that provide their services free of charge and operate on slim margins provide an example. Excessive requirements under NIS2 could force these free providers to exit the European market, creating the conditions for private certificate authorities to increase their prices. European businesses will face higher IT infrastructure costs, putting them at a disadvantage in comparison to foreign business that can still access these free services and have lower operating costs. This could have knock-on effects for European innovation and the ability of the European tech sector to compete globally.

Accountability

Accountability on the Internet gives users the assurance that organizations and institutions they interact with directly or indirectly are acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions.

DNS services are subject to layers of authority from state and community-led governance. For certain entities, confusion may exist as to which governance body holds authority, particularly when duplication occurs.

For example, to which authority would .tv, which is technically the ccTLD for Tuvalu but operates globally, be accountable? This problem would be particularly pronounced for ccTLDs that are strongly associated with sovereign nations. This ambiguity creates challenges for holding organizations responsible for their actions and providing transparency to the public.

The same question would apply to certificate authorities that operate globally and adhere to stringent requirements set by the Certification Authority Browser Forum (CA/Browser Forum)[23]. As the chain of authority becomes more complex, so does accountability for outcomes on the Internet, reducing transparency and trust.

Summary

The NIS2 would have negative consequences for four enablers, impacting the goal of an open, globally connected, secure and trustworthy Internet. By not supporting these enablers, the NIS2 limits collaborative development, management, and governance; unrestricted reachability; reliability, resilience, and availbility; as well as accountability.

Consequences could limit the development of future infrastructure that is optimized for users, the exit of essential DNS services from the European market, market consolidation and increased operating costs for EU businesses, and lack of acountability under conflicting sources of authority.

Conclusions

This Internet impact brief has identified several instances where the compromise proposal of NIS2 may harm or diminish the Internet as an open, globally connected, secure and trustworthy resource. The Internet Society recommends the European Commission conduct a full Internet impact assessment report to identify how NIS2 would impact DNS services, trust service providers, and certificate authorities as well as avoid any unintended consequences.

This report has also made several additional recommendations. This includes that root name servers should be explicitly excluded from the scope of the NIS2 proposal. Their inclusion in the proposal runs counter to historic EU support for a "single, open, neutral, free, secure and un-fragmented network". Regulating them would set the precedent for other governments to also impose regulation on the multistakeholder processes governed by the IETF and the Internet Architecture Board (IAB). Their inclusion could lead to the disintegration of common global identifiers, therefore increasing the risk of Internet fragmentation.

Additionally, this report recommends that the Commission encourage voluntary collaborative actions to strengthen Internet security and to protect data. Voluntary collaborative action for network operators helps to protect against route hijacking, route leaks, and IP address spoofing incidents. A voluntary model like the Internet Society's MANRS initiative, already adopted by more than 700 networks worldwide, can serve as an example.

[23] See: https://cabforum.org/ .