Body of European Regulators for Electronic Communications

BEREC

BoR (21) 60

BEREC Opinion on the proposed NIS 2 Directive and its effect on Electronic Communications

19 May, 2021

Contents

Abbreviations

CSIRT	Computer Security Incident Response Team
ECASEC	European Competent Authorities for Secure Electronic Communications (former ENISA Article 13a expert group) EECC European Electronic Communications Code Directive
ECN	Public Electronic Communications Network
ECS	Publicly available electronic communications services
ENISA	The European Union Agency for Cybersecurity
NRA	National Regulatory Authority (for electronic communications)
SPOC	Single Point of Contact

Executive summary

On 16 December 2020, the European Commission published a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 proposal) which (among other changes) foresees the inclusion of public electronic communication networks ("ECN") and services ("ECS") under its scope. The NIS 2 proposal suggests that the current security provisions in Articles 40 and 41 in the European Electronic Communications Code ("EECC") can be transferred to the NIS Directive by simply replacing them with similar provisions under Article 18 and 20 in the revised NIS Directive.

While BEREC recognizes that there is a rationale for the proposal to collect all critical infrastructures under one security framework, BEREC is deeply concerned about the effects of fragmenting the EECC. Further to this the concern goes to the effect of the proposed changes on the ECN and ECS markets as well as on the overall common security level reached with the targeted measures established since 2009 with the implementation of Art. 13a and 13b of the Framework Directive (now included as Art. 40/41 in the EECC).

In particular, BEREC has the following concerns with the NIS 2 proposal:

- The electronic communications sector already has its own sector specific comprehensive and proven regulatory framework that takes all perspectives into consideration including security, economic analysis, competition law and other regulatory issues. This holistic approach to the security of the electronic communications sector which has successfully adapted to the changing security landscape, has proven its merit. The sector cannot afford the risk of losing the experience with legal, technical and economic aspects of security in the current framework, built over 10 years.

- The electronic communications sector is a crucial sector in terms of security, because the functioning of other essential and important entities in other sectors depend on it; hence the electronic communications sector differs fundamentally from the entities in other sectors. This crucial role justified, and still justifies a separate regulatory approach.

- Some current definitions of the NIS 2 proposal are unclear (e.g. "security of networks and information systems") and not suitable with regards to the inclusion of the ECN and ECS;

Obligations foreseen in NIS 2 proposal may be disproportionate for some providers (e.g. small ones), acting as a barrier to market entry; In light of these concerns, BEREC considers it most appropriate to retain Articles 40 and 41 in the EECC and to not change and shift these provisions into the context of the NIS Directive

Should the European Institutions nevertheless seek to press ahead with the proposed change and shift of the relevant provision, BEREC strongly recommends that:

- Sufficient safeguards are introduced to the NIS 2 proposal to ensure the continuation of current practices and build on the knowledge and experience of current competent authorities for the security of ECN and ECS;

- The definition of ‘security of network and information systems’ in the NIS 2 proposal is reviewed and clarified.

Finally, BEREC further suggests to undertake a review of the NIS 2 proposal based on the assessments in this opinion, in order to better understand how the NIS 2 proposal could best complement the provisions in the EECC.

1. Introduction

On 16 December 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented, in a joint communication, "The EU's Cybersecurity Strategy for the Digital Decade"[1], which includes a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 proposal).

The BEREC 5G Cybersecurity ad-hoc Working Group[2] has prepared an independent BEREC opinion on the proposal. In this opinion, BEREC focuses on some key observations and possible impacts of the proposal on the public electronic communications networks and services.

2. Background

The security of public electronic communications networks and publicly available electronic communications services (hereafter ECN and ECS) has been regulated for over ten years using the existing regulatory framework in the field of electronic communications.

The Directive 2002/21/EC amended by the Directive 2009/140/EC[3] established provisions on security of ECN and ECS through Articles 13a and 13b. These Articles have been upgraded as Articles 40 and 41 of the EECC[4], setting out the measures that Member States have to put in place to ensure the security of public electronic communications networks and publicly available communication services, including stored or transmitted or processed data as well as any related services. The provisions also include responsibilities with regard to incident reporting and the implementation and enforcement of security measures. The provisions encompass the entire scope of possible security threats. This includes damage caused during civil works, natural phenomena, rodents, hacking, failed software or hardware updates.

[1] Joint communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

[2] Over the past years, BEREC has through its 5G Cybersecurity WG been involved in this work assisting the NIS Cooperation Group (NIS CG) and ENISA in their work related to network security and in particular, the EU Toolbox for cybersecurity of 5G networks implementation

[3] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services http://data.europa.eu/eli/dir/2009/140/oj

[4] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code http://data.europa.eu/eli/dir/2018/1972/oj

The implementation of the security provisions follows the general objectives of the EECC (defined in Article 3) in order to allow a consistent implementation of the regulatory framework. NRAs or other competent authorities have developed a set of national security requirements that providers of ECN and ECS must meet. These requirements are not only limited to the networks and the services offered, but also concern technical measures or measures ensuring the security of transmitted data, such as encryption and also with regard to billing, traffic and location.

The harmonisation of these security provisions is supported by ENISA through the ECASEC expert group. In ENISA's reporting of incidents over the past 10 years[5] approximately 65% of the incidents are related to system failures, 20% to human errors, one 10% to natural phenomena and only 5% to malicious actions. Cyberattacks such as hacking or distributed denial of service are a subset of malicious actions. The incidents with the largest impact in terms of user hours were mostly caused by system failures and natural phenomena.

The NIS Directive[6], adopted in 2016 and part of a wider EU Cybersecurity strategy, applied similar security provisions as those in Articles 13a and 13b of the Framework Directive to operators of essential services in other sectors, namely energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure (i.e. IXPs, DNS and TLD name registries). Under the NIS Directive, Member states designated a SPOC, national CSIRTs and competent authorities for the supervision and enforcement of the provisions in the national legislation. The security oversight of ECN and ECS was excluded from its scope and remained within the Framework Directive.

Following a recent review of the NIS Directive, the European Commission published its EU Cybersecurity Strategy on 16th December 2020, containing a proposal for a Directive on measures for a high, common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS)[7]. The NIS 2 proposal extends the scope of the NIS Directive to additional sectors within a framework distinguishing essential and important entities, including ECN and ECS (Annex I No. 8 of NIS 2 proposal). As a consequence, Article 40 of NIS 2 proposes to repeal Articles 40 and 41 of the EECC.

BEREC can understand why a horizontal cybersecurity approach across many and vastly different sectors could be beneficial if synergies between these sectors can be found. However, BEREC believes that the current proposal does not lead to such improvements for the specific sector of ECN and ECS.

---

[5] https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[7] https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

3. Assessment

This section compares the functioning of Articles 40 and 41 under the EECC to the equivalent articles under the NIS 2 proposal. In this assessment, various aspects will be considered to evaluate the changes from the NIS 2 proposal.

Assessment of the aims, objectives and mechanisms

BEREC notes that the aims, objectives and mechanisms of the NIS 2 Directive and the EECC differ and therefore the legal text comprising Articles 40 and 41 in the EECC and its equivalent under the NIS2 will have different impacts on the market.

The EECC has four general objectives of equal importance which are:

- promoting connectivity and access to very-high capacity networks;
- promoting competition and efficient investment including innovation;
- contributing to the development of the internal market and
- promoting the interests of the citizens of the Union.

These four objectives have also been guiding BEREC's work and should be taken into account in the decision-making of NRAs. Hence, the security aspects have a direct bearing on promoting the interests of the citizens. Additionally, security measures may also either directly or indirectly impact the other objectives of the EECC.

In order to reach the objectives set out in the EECC and at the same time abiding by the security provisions, it is necessary to apply the security measures in a proportionate manner. This is the underlying principle set out in Article 3 (1) of the EECC, which mandates the NRAs to always consider whether the intended regulatory measures are proportionate and reasonable with regard to the four objectives of the EECC. The principle of proportionality, on which the EECC is based, allows Member States thus to take appropriate and proportionate action as required, taking into account among others, the size of the undertaking or the number of users affected. Articles 40 and 41 are therefore meant to be assessed inevitably in conjunction with the proportionality principle set out in Article 3 of the EECC, with regard to *all* objectives. Conversely the NIS 2 proposal does not refer to objectives other than ensuring a high common level of cybersecurity as set out in Article 1 (1). Also, Article 2 (2) subjects public electronic communications networks or services "regardless of the size" of an entity to the application of the provisions. The measures set out in Art. 18 (1) of the NIS 2 proposal apply more stringently, irrespective of the sector. Thus, the two main advantages of Art. 40 and 41 EECC are lost – the holistic approach taking into account all objectives of the EECC as well as the sector specific approach where the consideration of different criteria allows for a more balanced and targeted regulation of security of electronic communications networks and services.

Security measures applied beyond the boundaries of proportionality can act as barriers to market entry or to remain in a market. This can have a negative effect on the functioning of a

competitive internal market and therefore on the end users. Cognizant of the balanced and holistic approach to regulation, apart from proportionality the EECC additionally provides various principles and mechanisms such as impartiality, public consultation processes and transparency. These collectively act as checks and balances to ensure efficient, proportionate and effective regulation.

BEREC identifies the following reasons not to integrate the electronic communications sector together with other sectors that are distinctly different in their nature into the NIS 2 proposal:

i. The electronic communications sector serves essential and important entities in other sectors as an “operational resource” and hence differs fundamentally from the entities in other sectors.

ii. The electronic communications sector already has its own comprehensive and proven sector-specific regulatory framework that takes all perspectives into consideration including security, economic analysis, competition law and regulatory principles.

Given these differences, a horizontal cross-sector approach is not optimal. Instead, having separate legal frameworks will allow a clear demarcation between the electronic communication sector under the EECC and the networks and information systems of other sectors under the horizontal approach of the NIS framework. Simply adding the security provisions related to the electronic communications sector under the NIS 2 proposal for the sake of having all relevant infrastructures under the same umbrella risks reducing the overall common security level reached with the targeted measures established since 2009 with the implementation of Art. 13a and 13b of the Framework Directive (now included as Art. 40/41 in the EECC).

Finally, examples of other provisions in the EECC to which the security provisions are interrelated would be in particular ensuring the availability of emergency communications and public warning systems and the development and secure deployment of new network technologies such as 5G and 6G.

The results of a survey of NRAs’ competencies carried out by the BEREC Cybersecurity 5G Working Group in February 2021 and presented in the Annex of this opinion show that while most NRAs are the competent authorities for the supervision and enforcement of the security provisions of ECN and ECS under the EECC (Articles 40 and 41), only a minority of NRAs are designated as SPOC, national CSIRT or competent authority under the NIS Directive. Where the NRA is designated as a competent authority under NIS, it is usually for the digital infrastructure sector or the digital service providers.

In order to avoid the loss of established practices, recital 49 of the NIS 2 proposal encourages the continuation of the application of the existing national regulatory framework for the telecom sector. However, the current wording in the recital is not clear and does not provide any guarantee that the advice is followed by Member States when transposing the Directive. Hence, BEREC believes that the risk for this loss of knowledge and experience remains.

Assessment of the definitions

Security provisions under the NIS 2 proposal are further different to those under Article 40 and 41 of the EECC due to differences in the definitions of both Directives.

The main difference arises in the NIS 2 proposal when it continues to use the definition of 'security of networks and information systems'[8] from the current NIS Directive and not aligning it with the definition contained in the EECC. Similar to the current NIS Directive, it is envisaged that the applicability of the NIS 2 proposal will be across many sectors. Therefore, it is understandable that the NIS 2 proposal requires more generic definitions to apply horizontally across the sectors envisaged within its scope rather than the sector specific definition of 'security of networks and services'[9] provided in the EECC. However, unless the definitions are aligned appropriately, there is a risk that necessary sector-specific applicability will be lost and may lead to misinterpretation.

BEREC identifies potential issues in the 'generic' definition of "security of network and information systems" as proposed in the NIS 2 proposal.

i. Under the EECC, the security regulation of ECN falls within the scope of Articles 40 and 41 irrespective of whether, when compromised, there is an impact on the data and related services offered by or accessible via this network. The EECC's definition of 'security of networks and services' includes electronic communications networks explicitly. This is not explicitly the case in the definition of 'security of networks and information systems' as set out in the NIS 2 proposal. Such non-alignment of the definition of 'security of networks and information systems' implies a possible gap compared to the Art. 40 and 41 EECC definition and risks losing the necessary sector-specific applicability of the NIS 2 proposal. Further, it risks misinterpretation of the applicability of the NIS 2 proposal to ECS and ECN and consequently a potential reduction to the intended scope and security level.

ii. The second issue arises from the use of the term 'related services' which is not defined and remains open to interpretation. The definition of 'security of networks and services' explicitly includes ECS. This is not the case in the definition of 'security of networks and information systems' in the NIS 2 proposal. Under the EECC, the services relevant

[8] 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

[9] 'security of networks and services' means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services;

to the network are clearly identified and defined as being the ECS. In fact, the definition of 'security of networks and services' in the EECC also includes a reference to 'related services' as the term is listed alongside "electronic communications networks and services" and "stored, transmitted or processed data", all of which can be compromised by an incident and hence their availability, authenticity, integrity or confidentiality have to be secured. The definition in the EECC also adds that "related services [are] offered by, or accessible via, those electronic communications networks or services". Due to the intertwining of the ECS and related services in this definition, a Member State can infer that the related services are rather ancillary to the "main" services offered by the ECN or ECS providers. Thus the difference in definition might lead to different interpretations and consequently indicate differences in scope. If this detail is lost in the definition used in the NIS 2 proposal, the scope and therefore the applicability of the NIS 2 proposal might be different.

As a consequence, there is a risk that some obligations provided for by the EECC will no longer exist if Articles 40 and 41 of the EECC are repealed as foreseen in the NIS 2 proposal. For instance, it remains unclear, if providers of ECS would still have the obligation to take appropriate and proportionate measures to prevent incidents affecting their services when they are not related to information systems or are not cyber-related.

The inevitable lack of clarity relating to these issues may lead to a reduced level of security as the generic definition cannot capture adequately and fully the specificities of the electronic communications sector. Hence, including the electronic communications sector under the NIS 2 proposal risks reducing the effectiveness of specific areas of supervision compared to the EECC.

Therefore, as long as this unclarity remains, repealing Articles 40 and 41 of the EECC may have significant impacts on the obligations currently imposed on some market players, especially providers of publicly available electronic communications services which may be subject only to obligations of a narrower scope according to the NIS 2 proposal.

Assessment of the motivation and consequences

The consolidation of existing legislation into a single legal instrument may introduce some advantages, however, this also comes with risks, if the existing and effective sector-specific aspects are not carried forward into the new legislation. Indeed, on assessing the proposal to move the security requirements of Articles 40 and 41 from the EECC to the NIS 2 proposal, BEREC can envisage a number of disadvantages, not least the inherent risk introduced by a generic and horizontal legislative tool, when compared to the existing sector-specific framework.

BEREC does not concur that removing the provisions concerning the security of ECN and ECS from the EECC would be an improvement for the security of the sector. The reasons presented in the impact assessment of the Commission do not provide a convincing

explanation as it is not explicitly considering the consequences of repealing Articles 40 and 41 from the EECC

As stated in recital 12 of the NIS 2 proposal, “sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking fully into account the specificities and complexities of those sectors”. The electronic communications sector consists mainly of private entities, which own and operate complex interconnected networks that are of great importance to society. A systematic approach to having an understanding and knowledge of the infrastructure and its development, monitoring obligations and ensuring compliance is vital to ensuring the security of ECN and ECS. As such, the proposal to repeal Article 40 is contrary to the argument presented in the recital 12.

Having separate legislative instruments is not hampering the work to improving the security and/or resilience of the electronic communications sector. An example for this would be the Commission Recommendation on Cybersecurity of 5G networks[10] and the subsequent publication of the EU Toolbox on Cybersecurity of 5G networks. At the same time, provisions under the EECC are deemed sufficient to address the technical objectives of the 5G toolbox, illustrating that the security provisions in both the EECC and the proposed NIS 2 Directive can co-exist and provide a holistic approach. Therefore (a) the benefits of the current context, and (b) the benefits the Commission is trying to pursue in proposing the repeal Articles 40 and 41 of the EECC, need to be reconsidered.

BEREC would caution against repealing Articles 40 and 41 from the EECC as there is a clear risk of losing the experience and benefits of the current framework built over 10 years’ experience, which has successfully adapted to the changing security landscape of the electronic communications sector.

4. Conclusions

On the basis of the analysis set out in section 3 above, BEREC is of the opinion that Articles 40 and 41 should be kept in the EECC rather than being repealed and replaced by the Articles 18 and 20 of the NIS 2 proposal which are out of context. BEREC considers the sector-specific approach in the EECC to be better suited than the horizontal approach of the NIS 2 proposal for the regulation of ECS and ECN. The NIS framework focuses on cyber security across multiple sectors, meaning the inclusion of ECN and ECS in its scope could lead to a risk that the security of ECN and ECS would not be adequately covered and therefore lead to a risk of significant gaps in oversight, ultimately leading to a reduced level of security of the electronic communications sector.

[10] Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335

Repealing Articles 40 and 41 EECC will additionally reduce the effective regulation of the electronic communications market because of the separation of the security provisions from the four objectives of the EECC and applying security regulation outside the comprehensive sector specific framework of the EECC.

It is important to have technical, economical and legal expertise in electronic communications to be able to appropriately and effectively regulate the security of ECN and ECS with a holistic approach.

There is a risk that the lack of clarity of the definitions may result in legal challenges in specific areas of supervision under the NIS 2 proposal compared to the EECC.

In the light of the argumentation above, BEREC finds:

- The electronic communications sector serves essential and important entities in other sectors as an “operational resource” and hence differs fundamentally from the entities in other sectors;
- Some current definitions of the NIS 2 proposal are unclear (e.g. “security of networks and information systems”) and not suitable with regard to the inclusion of the electronic communications sector of public networks and services;
- Obligations foreseen in the NIS 2 proposal may be disproportionate for some providers (e.g. small ones) acting as a barrier to market entry;.

In light of these concerns, BEREC considers it most appropriate to retain Articles 40 and 41 in the EECC.

Should the European Institutions nevertheless seek to press ahead with the proposed change and shift of the relevant provision, BEREC strongly recommends that:

- Sufficient safeguards are introduced to the NIS 2 proposal to ensure the continuation of current practices and build on the knowledge and experience of competent authorities for the security of ECN and ECS;
- The definition of ‘security of network and information systems’ in the NIS 2 proposal is reviewed and clarified.

Finally, BEREC further suggests to undertake a review of the NIS 2 proposal based on the assessments in this opinion, in order to better understand how the NIS 2 proposal could best complement the provisions in the EECC.

Annex 1 Survey results

In February 2021 the BEREC 5G Cybersecurity Working Group conducted a survey about the NIS-competences of NRAs under the current legal frameworks. On the questions whether the NRA is or will be competent, the NRA could answer 'Yes', 'Partially' or 'No'. The aggregated results of the answers of 27 participating NRAs on the survey are shown in the figure below.

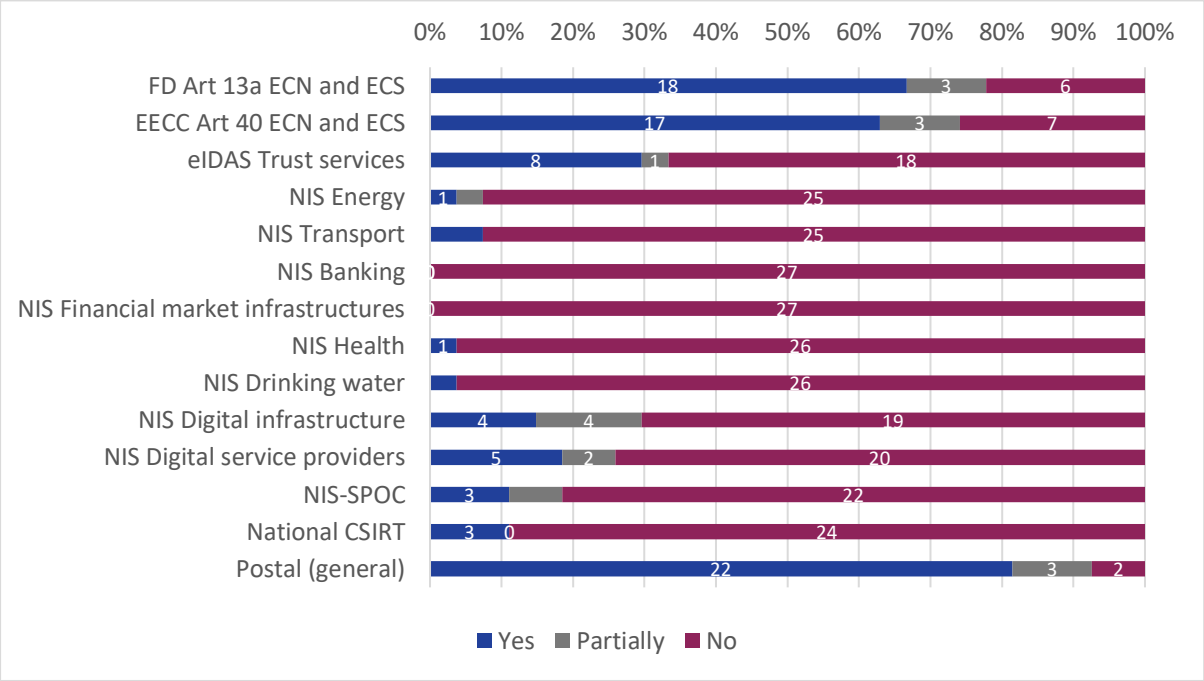

Figure 1: NIS-competences of NRAs under the current legal frameworks