CEER response to the Commission's public consultation on the priority list of Network Codes

14 May 2020

CEER welcomes the public consultation[1] to establish the priority list of Network Codes. Network Codes in general have proven to be a useful legal instrument for achieving steps towards an integrated EU energy market and for enhancing security of supply. Thus, the approach should in general be continued.

1 CEER response to the priorities regarding electricity networks rules for the period 2020-2023 (and beyond)

The need of a new electricity Network Code on cybersecurity

CEER believes that cybersecurity is crucial for the functioning of the EU's energy supply. Regulators observe that European energy companies have already made great efforts to secure their digital systems. This pertains not only to system operators, but also to the market side – such as trading companies and suppliers. Implemented security measures are either the result of industry initiatives or a reaction to cybersecurity regulations on national levels. In many cases however, the regulations are not energy-sector specific. Regulators fully support the continuation of efforts to maintain and enhance cybersecurity in the energy sector. Given the already-existing regulations at national levels issued in the adaption process of the NIS Directive or supplementing the EU Cybersecurity Act, or parts of the Clean Energy Package (e.g. best available technics for metering or cybersecurity in risk preparedness plans), any additional requirements coming from a cybersecurity Network Code should be properly justified and scoped.

CEER is of the opinion that a minimum level of cybersecurity is a prerequisite for the increase in data exchange necessary in the future to facilitate large-scale integration of renewable energy sources (RES). The possibility to open markets to new players, and to promote the role of active consumers (prosumers) and aggregators, also depend on well-functioning information technology. For this reason, cybersecurity is instrumental to the technological advancement of the energy markets. At the same time Regulators state that cost-efficient deployment based on adequate concepts and hardware is in the interest of all consumers.

The adequate scope of a new electricity Network Code on cybersecurity

CEER believes that the Energy Expert Cyber Security Platform (EECSP) report[2] of early 2017 and the Smart Grids Task Force (SGTF) EG2 report[3] of late 2019 are a good foundation for the further work on a cybersecurity Network Code. CEER wants to emphasize the following aspects:

1. **Evaluation of organisations in scope of the cybersecurity Network Code:** The scope illustrated by Figure 1 in the report of SGTF EG2 can be understood as meaning that only electricity grid operators should be in scope of the Network Code. CEER believes that also market players such as RCCs, NEMOs, operators of interconnectors, larger energy generators, industrial customers, aggregators, the balancing platforms as well as other relevant system infrastructure and actors in the power sector should be considered for the scope. In this way, it

[1] https://ec.europa.eu/energy/en/consultations/public-consultation-establish-priority-list-network-codes
[2] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
[3] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

will be ensured that all elements that are of significance for the functioning of the energy supply are taken into consideration for the Network Code.

2. **An "all hazards" cybersecurity approach for the energy sector:** CEER believes that a cybersecurity Network Code should follow an "all hazards" approach, meaning it should not only deal with protection against cyberattacks, but also cover events such as natural disasters, system errors and human mistakes. Some security aspects might be overlooked when discussing logical security, while they still should be part of a holistic cybersecurity approach. Examples on such aspects can be Physical Security, EMP-Security and Human Aspects like e.g. education and training.

3. **Cyber resilience for continuous energy supply:** One of the main conclusions of the EECSP report is that continuous improvement of cyber resilience should be a main strategic priority. CEER believes that the complexity that comes with the current technological development means we must assume that industry networks, at some point, will suffer compromises, system errors or other disruptive events. An entity's ability to continuously deliver the intended outcome despite adverse cyber events is known as "cyber resilience[4]". The effectiveness of a resilient infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event[5]. CEER believes that a key function of a Network Code on cybersecurity should be to safeguard cyber resilience for the energy supply.

4. **Technologies, processes and organisations as well as cost-efficiency:** The EECSP recommends a set-up that allows a holistic and effective cyber security treatment in the European Union. The energy sector consists of a variety of organisations that are different in size, differently organised, and have variations in both processes, responsibilities and technology solutions. CEER believes that a Network Code on cybersecurity must play together with the nuances of the technologies, processes and organisations, to avoid unnecessary spending on e.g. certification regimes or fulfilment of requirements that is not cost-effective.

5. **More diverse categories of cybersecurity measures:** The mere distinction between operators of essential services and operators of non-essential services, derived from the NIS classification, may be too restrictive and overly simple to be able to define what category of cybersecurity measures should apply to an organisation. By relating cybersecurity measures not only to two organisational levels, but also to the types and criticality of systems an organisation operate, measures can be more efficiently targeted. An example of this is the Network Code on Requirements for Generators[6] Article 5, which determines four levels of significance based on the voltage level of their connection point and their maximum capacity. Then, requirements are assigned, based on significance level.

6. **Key terms should be used with caution:** CEER recommends to not build in terms of the NIS directive, such as "Operator of Essential Services", into the future Network Codes. An organisation defined according to the NIS Directive as an Operator of Essential Services, e.g. an important market player, is not necessarily essential for the functioning of the energy supply. CEER understands it may be tempting to write a Network Code in a spirit that is compatible with the NIS Directive, but the respective rulesets should not concretely depend upon each other.

7. **Additional measures should be encouraged:** Organisations adhering to lower cybersecurity standards should be encouraged to apply more advanced cybersecurity standards. The encouragement may, for example, be via an adequate economic incentive system that can be implemented after proper metrics have been set for the purpose.

[4] https://en.wikipedia.org/wiki/Cyber_resilience
[5] https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2016_112_R_0001

8. **Extend the possible participation in early warning systems:** All organisations affected by the Network Code should be able to be part of early warning systems on a voluntary basis. Such early warning systems should include collecting, cleaning, validation and secure dissemination of relevant information to the entire energy system community without discrimination, allowing all stakeholders to benefit from the shared information about cybersecurity indications and alerts.

Given the potentially increasing importance of sector coupling in the future, CEER further recommends considering how cybersecurity could be ensured not only in the electricity sector, but also for gas(es) and other relevant energy sectors on which the electricity sector is highly dependent.

The need and adequate scope of new electricity Network Codes on demand side flexibility
Demand side response is already an important element of the European electricity system, and its relevance will increase with continuing deployment of volatile RES generation and the application of a range of flexibility solutions, including storage. The flexibility provided by demand needs to be well utilised in order to enable the already-started energy transition.

Flexibility should be seen with a wider lens, in the context of an integrated energy system which considers all forms of flexibility and takes into account the emergence of new technologies and new forms of gases. One should consider all points in the value chain and across all available energy vectors.

Many Member States already have systems in place which enable or foster the participation of demand in existing (market) mechanisms. This needs to be kept in mind as a starting point for the judgement on the necessity of a demand side flexibility Network Code. Moreover, existing Network Codes (in electricity such as Balancing and CACM) have a very strong emphasis on the provision of flexible resources including demand for system stability reasons. Any new legislation should not impede or hinder these already established processes, but rather build on them.

Finally, Regulators want to draw the attention to ongoing national legislation processes. A number of articles from the Electricity Directive (2019/944) such as Art. 17, Art. 32, Art. 36 are still to be transposed by Member States. Amongst others, these articles deal with issues which are highly relevant for the utilisation of demand side flexibility. It remains to be seen to what extent the legislative and implementation work will help to utilise the demand response flexibility potential, including across borders. In other words, any further integration via a new Network Code should be postponed until Member States have had the chance to implement the aforementioned articles into their national legislation. Furthermore, an evaluation of said implementation should first take place and the applicable process if it is detected that said implementation is not fulfilled would be infringement proceedings against those Member States.

Consequently, Regulators recommend to carefully follow, monitor and evaluate the ongoing processes regarding the utilisation of demand flexibility and Regulators offer, of course. full support to the relevant monitoring and design processes. Since the potential starting date for the work on a demand side flexibility Network Code is 2022, we do suggest taking a final decision on the need and the timing for such a Network Code closer to this date. As currently assessed, **Regulators do not find it necessary to produce a specific Network Code on this topic now.** Another important reason for having careful considerations on the timing is that in case a Network Code would be elaborated, it is likely that the emerging EU DSO entity would play a role in this elaboration process. Thus, this entity should be properly operational when this work commences, otherwise a pivotal actor could not give its crucial contribution.

The need and possible scope of new electricity Network Codes and guidelines that could be envisaged beyond 2023.
For the time horizon from 2023 onwards, the EU Green Deal will clearly shape the European Energy policy. This will also drive the need for new rules in some areas or require modifications in existing rules and Network Codes. Which areas should be covered will broadly depend on the precise directions of the Green Deal. Thus, Regulators recommend defining priorities for 2023 and beyond once the Green Deal becomes more specific. However, we would like to recall that this does not necessarily require new Network Codes but may also require significant modifications in existing ones.

2 CEER response to the priorities regarding gas networks rules for 2020 (and beyond)

As a general remark, CEER agrees with the European Commission that no new gas items should be included in the priority list for 2020. Implementation of the existing Network Codes, in particular the Gas Tariffs Network Code, remains a priority for national regulators. Furthermore, the impact of the implementation of the existing gas Network Codes on market functioning will need to continue to be monitored, with a view to identifying whether any issues persist and whether particular actions should be envisaged. In their November 2019 "Bridge Beyond 2025 Conclusions Paper,"[7] CEER and ACER outlined their proposals for a new system of dynamic and targeted regulation, with a process for monitoring and improving market performance going forward.

As noted in the Bridge Paper, the energy transition and evolution of our energy sector, including a move towards an integrated energy system, will require some reflection in the future regarding the legal and regulatory framework for gas(es).

In this regard, decarbonised gases should be able to be integrated into existing gas markets, with full valuation of their environmental benefits. However, it is important to highlight that decarbonised gases are only those produced from or using renewable energy. Hence, gases produced using electricity not coming from renewable energy cannot be considered decarbonised gases. Clear definitions and categorisation of decarbonised gases, including carbon capture and use or storage, should be established in European legislation, and consistent principles should be applied across the EU to facilitate the blending of decarbonised gases. Legislation should be sufficiently flexible to allow the emergence of new gases/technologies. At the same time, a technology-neutral, level playing field should be established between different conversion and storage facilities across the energy sector, so that they face equivalent categories of costs in network tariffs and levies, and equivalent recognition of environmental and security of supply benefits.

We must also foresee a clear regulatory framework and differentiation between competitive and monopoly activities. Transmission System Operators (TSOs) and Distribution System Operators (DSOs) should only be allowed to undertake potentially competitive activities under strict rules and as a last resort. In order to foster knowledge gain through application-based testing of innovative solutions, we propose to provide for an "EU umbrella" for a sandbox approach, allowing time-limited projects to be developed in which network operators shall not have a commercial role, with transparent clear rules and conditions which safeguard a competitive Internal Market. While it is too early to be definitive, large-scale hydrogen networks could be expected to provide regulated third party accessing. Similarly, an effective regulatory framework for infrastructure planning at EU level is needed to ensure a level playing field for new solutions, with a whole system, integrated, approach. The existing network operators face challenges from decentralised solutions and can no longer be regarded as completely neutral.

[7] https://www.ceer.eu/1767

In addition, and in light of recent concerns in this area, we believe that TSOs should consider developing harmonised counterparty risk management policy at European level and set up a centralised EU database on creditworthiness and market behaviour accessible to TSOs, NRAs, the Agency for the Cooperation of Energy Regulators (ACER) and the European Network of Transmission System Operators for gas (ENTSOG), in order to avoid that the costs of fraud and/or default are socialised. In parallel and to ensure that licensing requirements do not act as a barrier to entry, there should be mutual recognition across the EU of licensing for wholesale traders (or an equivalent mechanism). This should be accompanied by a mechanism for enforcement action, such as revoking the licence without undue delay if needed.

It may be that not all of these issues can or should be addressed in a Network Code, but we reiterate these points from the Bridge Conclusions Paper, as they may prove relevant in the European Commission's reflections on future actions.