Position paper

The Federal Ministry’s for Economic Affairs and Energy position paper on the ENTSO-E’s and EU DSO entity’s draft Network Code for cybersecurity aspects of cross-border electricity flows

The German Federal Ministry for Economic Affairs and Energy welcomes the ENTSO-E’s and EU DSO entity’s proposal for a Network Code for cybersecurity aspects of cross-border electricity flows (hereinafter “NC Cyber”). The Ministry shares the opinion voiced in the draft that sound cybersecurity requirements are crucial for maintaining security of electricity supply and ensure the highest level of cybersecurity in the electricity sector. Against the background of the increasing risk of cyber-attacks in the electricity sector, the introduction of appropriate cybersecurity measures is to be considered a priority.

However, the Ministry would want to make several remarks and would strongly suggest taking them into consideration during the further process.

1. Scope

Even though small and micro enterprises are excluded from the scope of the NC Cyber, at the same time the draft introduces the criteria "critical-impact" and "high-impact" entities. Should a small or micro-enterprise meet these criteria, it falls under the scope of the NC Cyber and must comply with all its requirements. The cybersecurity impact indices, which serve as basis for determining the critical-impact and high-impact, will be developed by ENTSO-E and EU DSO entity. However, several aspects of this process are unclear, e.g. which criteria and thresholds, including how they consider the cross-border electricity flows, would be taken into account while developing the indices and designing the process itself. It is also questionable whether ENTSO-E and EU DSO entity are legally entitled to develop such indices apart from the Network Code (a corresponding authorisation is missing in the Regulation 2019/943 (art. 30)) and what legal form, including its legal effect, such a document would have (ENTSO-E and EU DSO entity are not authorised to adopt binding legal acts) and whether the competent authorities would be bound by the indices. Furthermore, it remains unclear which national authorities will be responsible for determining the "critical-impact" and "high-impact" entities – while art. 2(2) provides for cooperation between the competent authorities for cybersecurity and the regulatory authorities, art. 27 only endows the competent authorities for cybersecurity with this task.

Due to these ambiguities, both the number and the circle of companies affected and thus the effects of the NC Cyber itself cannot be definitely determined. This includes possible competitive disadvantages caused by rising costs associated with implementation of the requirements. The scope of application of the NC Cyber must therefore be defined more clearly without referring to further elaborations.

2. Cooperation with other entities

A substantial part of the NC Cyber subsequent measures will be determined in cooperation with the "Cybersecurity risk working group". This exclusive group, which would consist of representatives of ENTSO-E, EU DSO entity, NEMOs and a limited number of main affected stakeholders, would largely develop the eligibility criteria to determine the “high-impact” and “critical-impact” perimeters and thus the affected enterprises as well as the other cyber security provisions to be fulfilled. The introduction of this working group is highly problematic, as it is not foreseeable which representatives of affected companies will be admitted as participants. Furthermore, neither the national nor the European authorities would be represented in the group, which means that they will have no influence on the elaborations, but will have to apply them. It is therefore necessary to provide a seat for the European (ACER/ENISA) and national authorities.

The same applies to the participation in the "Monitoring Body" that is to be established according to art. 16. It is necessary to enable participation of representatives of all national cybersecurity authorities and national regulatory authorities and not just some representatives of all authorities. Currently, the wording is unclear in this regard. Additionally, the results of the monitoring pursuant to art. 12 should be made available to not just the ECG as a subgroup of ESCO but also the NIS Cooperation Group (NIS CG), respectively the Workstream 8 (WS 8) of the NIS CG.

3. Conformity with the enabling provisions

Art. 59(2)(e) of the Regulation on the internal market for electricity (2019/943) empowers European Commission to adopt Network Codes addressing the cybersecurity aspects of cross-border electricity flows. Thus, the enabling legislation encompasses exclusively cross-border electricity flows. However, the provisions of the draft NC Cyber go beyond this enabling provision and refer also to electricity flows with no cross-border aspect. This becomes primarily apparent in the scope of the NC Cyber, which includes all DSOs and all electricity undertakings. As a consequence, all these companies are obliged to apply the NC Cyber regardless of whether they trade/transport electricity across the border as the particular provisions do not introduce any further differentiation. Furthermore, the proposal contains provisions that concern purely national electricity flows. Those provisions include art. 26 (Member States cybersecurity risk assessments), art. 43 (cybersecurity exercises at entity and Member State level), art. 45 (internal, national, regional or cross-regional cybersecurity exercises), Annex A (basic cybersecurity hygiene requirements), which lists requirements for all companies falling under the scope of the NC Cyber independent of the cross-border electricity flows. The expanded powers of the national competent authorities for cybersecurity (art. 34), which are to be endowed with the authority to inspect the companies concerned, go beyond the enabling provision, as they are not covered by any of the listed aspects of the enabling provision of art. 59(2)(e) (minimum requirements, planning, monitoring, reporting and crisis management). As a delegated act cannot go beyond the enabling provision, a deletion or an appropriate amendment is necessary. It is particularly important to clarify the scope of the NC Cyber so that it applies to cross-border electricity flows only.

4. Form of the legal act

The enabling provision in the basic act provides for the NC Cyber to be adopted in the form of a delegated act. Art. 290 (1) TFEU states that only non-essential elements of the relevant legislative act may be supplemented or amended by a delegated act. According to the ECJ’s established case law, "essential" within the meaning of art. 290 TFEU refers to provisions which are intended to give concrete shape to the fundamental guidelines of EU policy (ECJ, C-240/90, para. 37, Germany v. Commission). However, the draft of the Network Code contains several requirements which are "essential" elements of the act. This refers *inter alia* to art. 26 (Member State cybersecurity risk assessment) and art. 34 (cybersecurity inspections). Since these are essential aspects that do not involve amending or supplementing the basic act and impose substantial obligations on the Member States or give the authorities extensive powers, they should be adopted in the form of a regulation of the European Parliament and the Council (art. 288 TFEU). Therefore, these provisions should be deleted from the draft NC Cyber.

5. Consideration of the *Acquis communautaire*

The draft of the NC Cyber should take greater account of the existing European legal framework. This concerns *inter alia* definitions (art. 2) – instead of introducing new definitions, reference should be made to the existing ones (NIS2 Directive, ENISA-VO). In particular, greater reference should be made to the amendment of the NIS Directive (NIS2 Directive) regarding the scope and definitions, and its provisions should not be repeated in the NC Cyber (e.g. art. 37 – the role of the authorities responsible for cybersecurity, which was already defined in NIS2 Directive). Introducing new criticality criteria “critical-impact” and “high-impact” alongside the possibly varying criteria from the NIS2 Directive could be misleading. This also applies to other EU legal acts, such as the CER Directive and the AI Regulation, which introduce their own definitions of critical infrastructure. Rather, it is recommended to refer directly to the NIS2 Directive, especially in the area of cybersecurity. Furthermore, NC Cyber defines comprehensive tasks for the Computer security Incident Response Team (CSIRT) and adjusts them to the electricity sector. As the CSIRT is also relevant in other sectors, the tasks of the CSIRTS should rather apply equally to all sectors and should therefore be legally stipulated only in the NIS2 Directive. Therefore, it would be necessary to harmonise the two legal acts in order to provide clearer guidance for the companies and to increase the cybersecurity level. Therefore, it should be considered to delay the drafting of the NC Cyber with a view to the conclusion of the NIS2 Directive.

Furthermore, it should be ensured that the EU approach implemented at national level to apply the highest standards of security and "privacy by design" to the systems used to measure electricity supply (art. 20 b) Directive (EU) 2019/944) is not called into question. With regard to art. 35 (harmonising cybersecurity procurement requirements), it is particularly important that the high level of security required at national level with regard to the procurement and supply chains for smart meters for decentralized smart grids in the field of energy is not undermined.

6. Competences of the national authorities

The NC Cyber emphasises and even further strengthens the role and competences of the competent national authorities for cybersecurity when it comes to responsibility for implementing the measures provided for. However, the NC Cyber targets companies in the energy industry, for which, in principle, the regulatory authorities are responsible, that have fundamental knowledge of the sector, including the vulnerabilities the sector faces. It is therefore necessary to strengthen the role of the regulatory authorities and to involve them in the envisaged processes. Cooperation between the authorities should therefore be mandatory in determining the "critical-impact" and "high-impact" entities, monitoring and inspections. But at the same time, it is questionable whether the national regulatory authorities have the expertise to examine the regional risk treatment plans for their security under art. 21. At least an involvement or ideally an approval of the national authorities for cybersecurity would be necessary. A close cooperation of the competent authorities and continuous exchange of information should therefore be fostered, as this would enable the authorities to carry out their tasks effectively. In detail, such a close cooperation entails provisions of article 19 (2)(b) and (3)(c); article 26 (1), (2) and (3); article 27 (1) and (2); article 29; article 31; article 34; article 38; article 40 (2); article 43 and article 49 (5).

7. Disclosure of information

The draft of the NC Cyber provides in several provisions a compilation or even publication of information, which is to be considered sensitive. E. g. art. 2 (2) provides that the national authorities keep a list of micro and small sized enterprises or any other entities that are considered "critical-impact" or "high-impact" entities and accordingly to art. 27 (2) deliver a list of these entities to ENTSO-E and the EU DSO entity. Keeping a list of companies, which have processes which will or could cause disruptions in cross-border electricity flows, opens the door for potential cyber-attacks or threats to this companies and thus reduces cybersecurity instead of increasing it. This provision should therefore be deleted and other provisions re-evaluated on whether they would lead to publication of sensitive information. Instead, an exchange between the member states should be facilitated at the level of the national cybersecurity authorities. Sensitive data should then be aggregated and only the data necessary for the completion of the respective task should be provided to ENTSO-E.

8. Deadlines

The draft NC Cyber provides very short deadlines, which in this form are not suitable to foster cybersecurity but might on the contrary even lower it. The administrative burden of a bi-annual turn is considered to be overbearing. Especially in light of a tense job market for cybersecurity specialist, companies might be inclined to reduce their operational cybersecurity resources in order to fulfil the administrative requirements. In Germany, a three-year turn has proven to be sufficient and the control of cybersecurity has shown to be effective, as the tri-annual turn reduces the bureaucratic burden for the competent authorities. Additionally, extending the deadline to three years, would also align it with the gas sector’s deadlines, which would reduce the administrative burden of entities active in both sectors.

9. Zero-day vulnerabilities

The German Ministry cannot support withholding information about zero-day vulnerabilities, as stipulated in art. 37(5). Regardless of whether the respective manufacturer has developed patches or instructions at the time the vulnerability becomes known, mitigation methods may already have been developed independently of the manufacturer. In order to increase information security, the competent national authorities for cybersecurity and especially the CSIRT must be allowed to share this information independently of the manufacturer.