ALL NEMO COMMITTEE

NEMO Committee's answer to the ENTSO-E's consultation on Network Code on Cybersecurity

19/01/2022

1 General provisions

Q7: Are the objectives of the Network Code on Cybersecurity, which lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management sufficiently clear?
A: No.

Q: If your answer is "No", please elaborate:
A: The full objectives of the Network Code are not clear unless the exact scope of application of the Network Code is clarified.
The Network code risks to overlap with other cybersecurity-specific legislation, such as NIS 2. It is not clear how these different cybersecurity legislations would interact, and therefore what their respective objectives are. Also, these proposals will be implemented according to different timeframes, creating additional layers of complexity for entities to comply with the obligations of the legislation.
It should be clearer that rules on common minimum requirements, planning, monitoring, reporting and crisis management apply only to activities directly related to cross border electricity flows and do not overlap with existing cybersecurity legislation (NIS/NIS2), particularly considering that the NIS review will not be complete by the time this new Network Code is to be implemented.

Q8: The NCCS states: "Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation." Based on the statement above, are twelve months a reasonable timeframe?
A: No.

Q: If your answer is "No", please elaborate:
A: We believe that at this point in time, without knowing which entities precisely will fall under the scope of this Network Code, it is not possible to establish whether or not the timeframe is adequate.

Q9: The NCCS states: "Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation." Based on the statement above, do you think these requirements for small and micro enterprises are of sufficient level?
A: No opinion.

Q: If your answer is "They are too strict" or " They are too flexible, more strict requirements should be in place", please elaborate:
A: In NEMOs understanding the concept of SME will have no impact on NEMOs treatment since all NEMOs will be treated in the same way, as critical or high impact entities, regardless their size.

Q10: Do you consider the Monitoring approach defined at Article 12 to be effective to monitor the adequacy of the Network Code to the ever-changing technology landscape and evolution of applicable cybersecurity standards?
A: No.

Q: If your answer is "No", please elaborate:
A: The operational impact from the monitoring provision shall be kept reasonable and minimised. For example, the wording of Art. 12(3) of the Network Code should be amended to require that the methodology to be drafted by ACER is adequate, imposes the least degree of communication and information requirements and does not go beyond what is necessary for the purpose of the monitoring.
While information can be requested from any entity within the scope of the Network Code pursuant to Art. 12(6), only ENTSO-E and the EU DSO Entity would be consulted on the methodology for the collection of the information and are entitled to suggest amendments to the methodology as stipulated in Art. 12(3). We therefore suggest amending Art. 12(3) to allow for proper stakeholder consultation of all entities concerned as well as the explicit right to propose amendments for all entities in scope.
The data collection process of the new Network Code must be harmonised with existing legislation to avoid duplication of efforts in reporting. Additionally, a high level of security between ACER and national entities must be ensured to protect sensitive data.

Q11: Do you think the Benchmarking approach, as described in Article 13, is an adequate tool to assess whether current investments in cybersecurity to protect cross-border electricity flows are sufficient?
A: No.

Q: If your answer is "No", please elaborate:
A: Art. 13 must be carefully assessed to ensure that differences between Member States are sufficiently considered to allow for a meaningful comparison of data. For example, there can be a wide gap between Member States in the cost of labour which, if simply taken at face value, could be misleading when determining the cybersecurity investment needed to implement the new Network Code. Furthermore, we find that more clarity is needed on how the benchmarking process will impact cost recovery, e.g. if the correlation between the level of spending and the maturity of the sector (prudence of cybersecurity expenditure) does not reach certain efficiency thresholds. Will these entities be entitled to full cost recovery for the extra costs incurred?

Q12: Do the overall timelines within the Network Code on Cybersecurity seem reasonable?
A: No.

Q: If your answer is "No", please elaborate:
A: Regarding the timeline for the development and adoption of the new Network Code and its accompanying methodologies, more time is needed to ensure a sound and coherent rule set is being formed, agreed and established. Regarding the timeline for implementation, it is important to allow for sufficient time to ensure a smooth operational, IT and legal deployment of the new rules. The

measures adopted during the transition period must not simply be interim measures that are to be replaced by different obligations later on. Complex and costly interim measures may take resources away from the
implementation of an enduring solution.

2 Governance for cybersecurity risk management

Q13: Is it reasonable that the entities involved can perform the following tasks within the time set in the network code, given resource, capability, or other constraints?

Activities led by the CS-NCA and NRA:

a) **CS-NCA and NRA to perform the member state risk assessment within 3 months (Article X)**
b) **CS-NCA and NRA to make a transitional list of high-impact and critical-impact entities within 6 months after receiving the transitional ECII (Article Y)**
c) **CS-NCA and NRA to identify high-impact and critical-impact entities within 6 months after receiving the ECII (Article Z)**

Activities performed by entities:

d) **High-impact and critical-impact entities to report the results of their risk assessment in 6 months**
e) **High-impact and critical-impact entities to implement the minimum and advanced cybersecurity controls in 6 months after their publication**
f) **High-impact and critical-impact entities to provide evidence of verification of the controls in 24 months after their publication**

A: No per activity

Q: Do you have any additional comments on the timelines:

A: It is unclear to NEMOs whether this type of activity should be done by NEMOs individually or as common activity as part of being the MCO function. This distinction can have a clear impact on the timeline.

Q14: Is the proposed governance for cybersecurity risk assessment clearly described and sufficient to meet the objectives of the network code on cybersecurity?

A: No.

Q: If your answer is "No", please elaborate:

A: The governance of the Working Group established pursuant to art. 15 of the network code is lacking a decision-making procedure for the adoption of the methodologies. Additionaly, the Working Group shall be the body entitled to adopt the methodologies instead of being a support group to ENTSOE/EU
DSO who ultimately adopt all methodologies. Consequently, all stakeholders involved in the Working Group shall have the right to vote on the decision for approval of the methodologies. The decision-making process shall be at unanimity. The Working Group shall be established as the body

adopting the methodologies. The current governance proposal sets in stone throughout the articles of the network code many deliverables (e.g methodologies) to be established by the parties. It creates the risk of an unflexible framework for deliverables that may be deemed not necessary in the future. The governance shall establish that the Working Group is the body tasked ultimately with the decision to develop or not a methodology according to the need.

3 Risk management at Union and regional level

Q15: Under the network code draft, cybersecurity risk assessments are performed at four levels: Union-wide, regional, member state, and entity. By integrating information from these four levels, it should be possible to get a comprehensive view on the risks. How effective do you think this multi-level process will be in assessing and reducing the cross-border cybersecurity risks in the European electricity sector?
A: Effective

Q: If you think the process is not effective, how can it be improved?
A: Four levels seem efficient provided that there are no duplications of regulation in the Electricity sector.

Q: How do you think the efficiency of the risk assessment process could be improved?
A: Avoid duplication of obligations to be efficient.

Q16: The proposed scope of the cybersecurity risk assessments is the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. Legal, financial or reputational damage of cyber-attacks are out of scope. Do you think this is a good scope to manage the cybersecurity risks to cross-border electricity flows?
A: Yes.

Q17: Under the proposed cybersecurity risk management process, ENTSO-E and EU DSO with the RCCs make and approve a risk treatment plan. In approving the plan, they could be seen to accept the residual risks. Do you think this is an appropriate process for accepting the residual risks?
A: Yes.

Q: If not, which party should be responsible for accepting the residual risk at regional level?
A: In principle, we would find this to be an appropriate process provided that it is transparent and consults the opinion of stakeholders.

Q18: Is the proposed risk management at union and regional level clearly described and sufficient to meet the objectives of the network code on cybersecurity?
A: Yes.

4 Common electricity cybersecurity framework

Q19: Are the minimum cybersecurity controls for supply chain security in Article 24 (2) clear and sufficient?
A: No.

> **Q: If not, how should they be amended?**
> A: With respect to NEMOs, it could apply both at individual entity level and also at NEMO common functions level. There needs to be alignment with other legislation to avoid double obligations and inconsistencies.

Q20: The supply chain controls now require entities procuring new products and systems to set and enforce security requirements to suppliers. Should the network code also include controls that directly require suppliers to take certain measures?
A: No opinion.

Q21: The network code proposes cybersecurity hygiene requirements in Annex A to ensure that all entities that can affect the cybersecurity of the electricity grid have a baseline security. Do you think the proposed hygiene requirements are appropriate for reducing cross-border cybersecurity risks?
A: No opinion.

Q22: Is the proposed common electricity cybersecurity framework clearly described and sufficient to meet the objectives of the network code on cybersecurity?
A: No.

> **Q: If your answer is "No", please write what could be improved:**
> At this point in time, without knowing which entities precisely will fall under the scope of the new Network Code, it is not possible to establish whether or not the framework can meet the objectives.

5 Risk management at member state level

Q23: CS-NCA and NRA can appoint entities as high-impact or critical-impact even where they do not individually meet the ECII level. This allows them to appoint entities for which the aggregate impact of a group of similar entities is above the high-impact or critical-impact thresholds. Do you agree with this mechanism for dealing with groups of similar entities?
A: No opinion.

> **Q: If not, what mechanism should be used to deal with groups of entities?**
> A: In NEMOs understanding all NEMOs shall be treated in the same category, as critical or high impact entities.

Q24: Is the proposed risk management at member state level clearly described and sufficient to meet the objectives of the network code on cybersecurity?
A: No.

Q: If your answer is "No", what could be improved?":
A: Many NEMOs are designated in more than one member state. (Multi NEMO-Arrangements - MNA) It therefore need to be clear with which member state authorities the NEMO shall refer to. (The matter of coherence among obligations in different member states.)

6 Risk management at entity level

Q25: In Article 31, the network code requires entities to report information about existing controls, threats and vulnerabilities to their national regulators (CS-NCA and NRA). The regulators then report this information to ENTSO-E and the EU DSO entity for the regional risk assessment (Article 26). The information will give a good and detailed view of the cybersecurity risks to cross-border electricity flow. But the information could also be exploited by potential threat actors if they could obtain it. Do you think the benefit of collecting the information will be large enough to outweigh the risk of the information being compromised?
A: No.

Q: If your answer is "No", what changes would you propose?:
A: Both for information security reasons and the simplification of obligations, entities should have only one point of contact for reporting.

Q26: Entities determine the scope of the entity level risk assessment based on the outcomes of the Union-wide risk assessment, in particular the list of Union-wide high-impact and critical-impact processes. Do you think the process for determining the entity-level risk assessment scope is clear, and that the scope will cover all assets the entity needs to support cross-border electricity flows?
A: Yes.

Q27: The network code allows the CS-NCA and NRA to give derogations based on three criteria:

a) **in exceptional circumstances, when the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefit;**
b) **The entity can provide a risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable according to the risk acceptance criteria pursuant to Article 25.3.b. The risk treatment plan shall be verified through one of the options pursuant to Article 33.**
c) **The results of the risk assessment of the entity do not show any direct or indirect impact on cross-border electricity flows. Do you agree with the criteria and process for providing derogations?**

A: No.

Q: If not, how can the derogation process be improved?:
A: We believe that to ensure a level playing field and a common minimum level of cybersecurity standards, it must be ensured that entities using the same systems are covered by the NC to the same extent. If a derogation is granted, it must apply to all entities using the same system.

Q28: Is the proposed risk management at entity level clearly described and sufficient to meet the objectives of the network code on cybersecurity?
A: No.

Q: If your answer is "No", what could be improved?:
A: Article 29.2(d) should say "residual risk acceptance". Also, 6 months after entry into force may be too little time for entities to apply the minimum cybersecurity controls, as defined in Article 30.1. 24 months are more realistic. Article 34.6 should specify that random checks may only occur 24 months after entry into force of the network code.

7 Harmonising product and system requirements and verification

Q29: Is the proposed approach for harmonizing the cybersecurity procurement requirements and verification schemes clearly described and sufficient to meet the objectives of the network code on cybersecurity?
A: Yes.

8 Essential information flows, incident and crisis management

Q30: Article 37 request CS-NCA to provide electricity entities with information on cybersecurity incidents, threats, and vulnerabilities to enhance the electricity entities' defense. Do you agree that the network code will help electricity entities to receive effective and adequate information to increase their threat awareness and ability to handle cybersecurity incidents?
A: Yes.

Q31: Article 39 and Article 40 present the support electricity entities receive in the event of an incident (Art.39) and crisis (Art.40). Do you think that enough support is provided?
A: No.

Q: If your answer is "No", how should the support be reinforced?:
A: It is difficult to say if enough support is provided, as the exact obligations aren't clear and neither the exact scope of entities which will have to comply with this reporting is clear. (see also answer to

question 7). Also, in Article 39 (5) (d) the yearly frequency is not aligned with Article 43, where it states "every three years", which seems more reasonable.

Q32: Is the proposed approach for essential information flows and crisis management clearly described and sufficient to meet the objectives of the network code on cybersecurity?
A: No.

Q: If your answer is "No", what could be improved?:
A: Information protection must be more clearly described (for instance, why are the transitional lists for high and critical risk entities published on EU, DSO and Entso-e websites? They should be confidential).

9 Electricity cybersecurity exercise framework

Q33: Article 41 requires critical entities to perform two exercises every three years. Do you have the capabilities to perform the mandatory cybersecurity exercises?
A: No.

Q: If your answer is "No", how frequently should exercises be held?:
A: We fully support that essential electricity undertakings take part in cybersecurity exercises to detect issues and share best practices. However, these exercise scenarios should be tailored to each entity to ensure the right focus areas are being tested and to limit unnecessary resource expenditure.

Q34: Is the proposed electricity cybersecurity exercise framework clearly described and sufficient to meet the objectives of the network code on cybersecurity?
A: No.

Q: If your answer is "No", what could be improved?:
A: Exercises should be well coordinated to ensure that there are no overlaps - for example, regional and national exercises interfering with each other. Additionally, clear and long term planning (3-4 years ahead) is needed for predictability.

10 Protection of information exchanged in the context of data processing

Q35: Are the principles and implementation rules for protection of information adequate to protect classified and sensitive information to be exchanged in a trusted way?
A: No.

Q: If your answer is "No", which principles and/or implementation rules should be removed, added or modified?:

A: The new Network Code must explicitly mention that the list of critical risk entities, the list of identified critical parameters and systems, the cross-border electricity cybersecurity risk assessment report as well as the common electricity cybersecurity framework are European Union Classified Information
(EUCI) or the applicable equivalent national classification. This information shall be protected according to Title X (Arts. 46(5)(a)) and 47(4)) and not be made available publicly (e.g. on websites), to reduce the risk of malicious actors getting access to this information. Furthermore, based on Art. 49(8) it seems that entities "shall strive to progressively apply the standards and controls included in the transitional list of international standards and controls", while previously the understanding was that entities may apply either standards (as per Art. 49(6)(a)) or the set of equivalent controls as per Art. 49(6)(b).

Q36: Is the proposed protection of information exchanged in the context of this data processing clearly described and sufficient to meet the objectives of the network code on cybersecurity?

A: No.

Q: If your answer is "No", what could be improved?:

A: The network code shall explicitly mention that the list of high- and critical risk entities and the results of their risk assessments shall not be publicly available and shall be protected at minimum by a two-factor.

General

Q37: Do you see any areas where the network code on cybersecurity can be aligned better with the revised NIS directive now under development?

Please elaborate:

A: The full scope of the new Network Code remains unclear and leaves too much room for interpretation. We find that the material scope (i.e which activities performed by a given entity fall within scope) is missing and there should be explicit mention that only activities which pertain to cross-border electricity flows are in scope.

We further propose to add a new Art. 2(5) stating that entities providing services in several member states are supervised by a single regulatory authority of the country of establishment. For entities not established in the EU, the competent regulatory authority shall be the one of the Member State of the designated representative of the non-EU entity.

Further clarification is needed on cost recovery for all entities in scope. In particular, NEMOs should be able to recover their full costs.

Proposal: The costs borne by system operators subject to network tariff regulation and the costs borne by other electricity entities in scope stemming from the obligations set out in the present Network Code shall be assessed by the relevant regulatory authorities. Costs deemed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms for the system operators and for the other electricity entities through the system operators.

A definition of "sensitive information" is missing.

Art. 15.4 (new) ENTSO-E and EU DSO entity shall justify in writing to ACER and the Electricity Coordination Group any deviation from the proposals and analysis prepared by the cybersecurity risk working group.