WindEurope Response to ENTSO-E Public Consultation on Cybersecurity Risk Assessment Methodologies for the Network Code on Cybersecurity

Overview

Under Article 18 of the Network Code for Cybersecurity (NCCS), the European Network of Transmission System Operators for Electricity (ENTSO-E) in cooperation with the EU DSO entity (DSO Entity) has developed a proposal for methodologies for cybersecurity risk assessment. The document contains methodologies for risk assessments at three levels: the Union-wide risk assessment, the regional risk assessment, and the risk assessment at member state. No methodology is defined for risk assessments at entity level, as the entities may choose their own methodology if it complies with Article 26 of the NCCS.

The methodology, as stated in the NCCS, considers only the consequences to the grid's operational security of cyber-attacks at each level. The aim of these methodologies is to ensure the consistent assessment of risk across the different levels defined by the NCCS.

Questions

Completeness

Title 2 describes the Methodology for the Union-wide Cybersecurity Risk Assessment. Is the Methodology clear and understandable?

Yes.

The provisions for TSO and DSO are clear; however, there is ambiguity regarding the appointment of critical entities, which will occur at a later stage. Article 1(3) currently focuses on attempts with malicious intent to gain access to network and information systems. To ensure comprehensive protection, it should also explicitly address disruptions, such as denial-of-service (DoS) attacks, that affect the availability of these systems.

1. Title 2 describes the Methodology for the Union-wide Cybersecurity risk assessment. Does the Methodology meet all requirements and objectives for the Union-wide Risk Assessment in the NCCS?

No.

If not, please explain how the Member State Risk Assessment Methodology can be improved:

• Non-Malicious Cybersecurity Incidents: The assessments focus solely on consequences of cyber-attacks with malicious intent and do not consider cybersecurity incidents caused by threats with no malicious intent.

• Detailed Implementation Timeline: While there is a mention of an implementation timeline, more detailed steps and milestones could be beneficial for clarity.

• Stakeholder Consultation: Although there is a mention of consultation with the NIS Cooperation Group, more detailed information on the consultation process and stakeholder involvement could enhance transparency.

It is unclear the mention of measuring how many entities and attackers could attack at same time, and it is recommended to replace with a threshold of entities impacted by a cyberattack

2. Title 3 describes the Methodology for the regional Cybersecurity Risk Assessment. Is the Methodology clear and understandable?

   Yes.

3. Title 3 describes the methodology for the regional Cybersecurity risk assessment. Does the Methodology meet all requirements and objectives for the regional Risk Assessment in the NCCS?

   No.
   If not, please explain how the Member State Risk Assessment Methodology can be improved:

   • Legal, Financial, or Reputational Damage: The current methodology for cybersecurity risk assessments only considers consequences to the operational security of the grid and does not consider legal, financial, or reputational damage.

   • Non-Malicious Cybersecurity Incidents: The assessments focus solely on consequences of cyber-attacks with malicious intent and do not consider cybersecurity incidents caused by threats with no malicious intent.

   • Detailed Implementation Timeline: While there is a mention of an implementation timeline, more detailed steps and milestones could be beneficial for clarity.

• Stakeholder Consultation: Although there is a mention of consultation with the NIS Cooperation Group, more detailed information on the consultation process and stakeholder involvement could enhance transparency.

4. Title 4 describes the Methodology for the Member State Risk Assessment. Is the Methodology clear and understandable?

   Yes.

   Suggestions for Improvement:

   Article 16 (3) and Article 16 (6) appear as duplicate: (3) When reporting the risk of a compromise of availability, the competent authority shall report the outage duration that corresponds to the reported risk. (6) When entities report the risk of a compromise of availability, the competent authority shall require them to report the outage duration that corresponds to the reported risk. Currently there are no timelines mentioned for the different requests and no timelines for entities to reply within.

5. Title 4 describes the Methodology for the Member State Cybersecurity Risk Assessment. Does the Methodology meet all requirements and objectives for the Member State Risk Assessment in the NCCS?

   No.
   If not, please explain how the Member State Risk Assessment Methodology can be improved:

   • Legal, Financial, and Reputational Risks: The existing approach to cybersecurity risk assessments focuses solely on operational security impacts to the grid and overlooks potential legal, financial, and reputational consequences.

   • Non-Malicious Cybersecurity Events: The assessments emphasize the outcomes of cyber-attacks with malicious intent, neglecting incidents that stem from non-malicious threats or unintended actions.

   Comprehensive Implementation Timeline: While an implementation timeline is referenced, a more granular breakdown of steps and milestones would provide greater clarity and guidance.
   • Enhanced Stakeholder Engagement: Although the involvement of the NIS Cooperation Group is noted, offering more detail about the consultation process

and the participation of various stakeholders would improve transparency and inclusiveness.
• Common Minimum Requirements: The regulation should include more detailed rules on common minimum requirements for cybersecurity across the electricity sector.
• Planning, Monitoring, Reporting, and Crisis Management: There should be more comprehensive guidelines on planning, monitoring, reporting, and crisis management to ensure a high level of cybersecurity.
• Coordination with ENISA and ACER: The role of the European Union Agency for Cybersecurity (ENISA) and the Agency for the Cooperation of Energy Regulators (ACER) in the implementation and monitoring of the cybersecurity measures could be further detailed.

6. Annex I contains a list of metrics to measure the impact of cyber-attacks on the European electricity system. As stated in the NCCS, the risk assessments shall not consider the legal, financial or reputational damage of cyber-attacks. Are the impact metrics clearly defined?

   Yes.

7. Annex I contains a list of metrics to measure the impact of cyber-attacks on the European electricity system. As stated in the NCCS, the risk assessments shall not consider the legal, financial or reputational damage of cyber-attacks. Do the impact metrics cover all relevant impacts?

   Yes.

8. Annex III contains a list of threats that need to be considered in the Risk Assessments at all levels. Is the list of threats clear?

   No.
   Annex III describes ‘threats. –the naming of this annex is wrong (and the subsequent references to this annex). Annex III describes ways that a hostile threat actors can attempt to access a digital system to cause an impact to a process. We suggest changing the Annex and references to its topic in to ‘attack vectors’

9. Annex III contains a list of threats that need to be considered in the risk assessments at all levels. Are all relevant threats included?

   No.
   If not, please explain how the list of threats can be improved

The used attack vectors catalogue in annex III does not include all attack vectors and as result: - it will give a false sense of knowledge, - fail to address all risk. - Grow stagnant, and incapable of addressing newly developed hacker techniques Suggestion: Allow for multiple reference to public tools for attack vector analysis: Mitre Attack framework or ENISA threat catalogue

Sensitivity of information

10. How confidential would you consider the information that competent authorities report to ENTSO-E and the DSO Entity in the Member State Risk Assessment?

    EU Restricted

11. If you consider the information highly sensitive, how can we mitigate the risk of Member States sharing such information?

    1. Definition of Sensitivity: Sensitivity is determined based on its potential impact on national security. In alignment with TEUF Article 346, this requires adherence to 27 distinct aggregation methods, tailored to each member state.
    2. Mitigation Measures for Handling Sensitive Information To mitigate risks associated with sensitive information:
       o Confidentiality Agreements: All parties involved in the reporting process should sign strict confidentiality agreements, legally binding them to protect sensitive information.
       o Secure Communication Channels: Use encrypted and secure communication methods, such as 7zip or other encryption techniques validated by member states, to safeguard information during transmission and prevent unauthorized access.
       o Regular Audits: Conduct periodic audits to ensure compliance with confidentiality agreements and the effectiveness of access control measures

Aggregation Methods

12. What methods do you think should be used to aggregate the results of the entity level Risk Assessments for the Member State Risk Assessment?

    Aggregation Methods: Risk Assessment and Communication Requirements
    • Effective quantitative risk assessment is essential to ensure seamless communication within the supply chain and with authorities.
    • Power operators must have access to the same information from their suppliers as the authorities, ensuring transparency and consistency. Suggestions for Enhancing Risk Assessment and Reporting

• Facilitation by ENTSO-E: ENTSO-E should support the development of quantitative risk assessment methodologies. These methodologies should be practical for entities, fostering consistent reporting and alignment across the electricity industry.
• Addressing Double Reporting: The reporting format should mitigate the challenge of double reporting. Service providers designated as critical entities may need to report risks both directly to authorities and to their customers. The format should streamline risk aggregation to address this issue within the supply chain. Mitigation Measures for protecting sensitive information
• Confidentiality Agreements: Ensure all parties in the reporting process sign strict confidentiality agreements, legally binding them to safeguard sensitive information.
• Secure Communication Channels: Use encrypted and secure communication methods (e.g., 7zip or other state-validated encryption techniques) to prevent unauthorized access during information transmission.
• Regular Audits: Conduct periodic audits to ensure compliance with confidentiality agreements and the effectiveness of access control measures.

13. What methods do you think should be used to aggregate the results of the Member State Risk Assessments for the regional Risk Assessment?

Quantitative methods

Duration

14. The impact and risk of a loss of availability of information depends on how long the information is not available. In the Union-wide Risk Assessment, ENTSO-E and the DSO Entity will determine for each process the relevant duration over which a loss of availability should be analysed (see Article 5(3)). Entities currently, however, do not have to use the recommended duration in the Risk Assessment at entity level, as they may already be performing assessments with a different duration. Using different durations may, however, make it more difficult to aggregate the results at Member State level. Should entities be required to use the duration determined in the Union-wide Risk Assessment during the entity-level Risk Assessment when assessing the risk of a compromise of availability?

Yes.

Any sound risk assessment methodology should be data-driven, and as result the change in such parameters should not imply a heavy burden.

Thresholds

15. Annex II contains high-impact and critical-impact thresholds to be used in the Union-wide, regional and Member State Risk Assessments. Do the thresholds correctly classify if the consequences of cyber-attacks are of high- or critical-impact to the European electricity system?

    No.
    If not, please explain how the thresholds can be improved.

    To be efficient in detecting specific threats (i.e. third-party hacking on multiple actors connected with cross border electricity flows, Thresholds should be lowered.

Entity Reporting Template (Annex IV)

16. Annex IV and V contain reporting templates for the Risk Assessments at entity and Member State level. Are the reporting templates complete and at the right level of detail?

    No.
    If not, please explain which fields you would like to add or remove:

    To ensure coherence across regions and entities in reporting, a minimum list of mandatory processes should be provided, enabling more efficient union-level analysis. To ensure coherence across regions and entities in reporting, a minimum list of mandatory processes should be provided, enabling more efficient Union-level analysis. However, while the adoption of standards such as ISO 2700X and IEC 62443 can provide valuable frameworks for cybersecurity risk management, it is important to treat these standards as normative guidance rather than prescriptive requirements. This approach ensures the flexibility essential for tailoring risk assessments to specific organizational and regional needs while supporting harmonization with diverse cybersecurity laws and regulations. Specific improvements include clarifying the concept of residual risk in Article 16 (2)(c), refining Article 16 (4)(b) to emphasize that monitoring controls must address specific risks and renaming Annex III from "threats" to "attack vectors" to reflect its content more accurately. Additionally, the sensitive nature of entity-specific risk registers in Annex IV warrants careful handling. For Managed Security Service Providers and critical ICT service providers, the "Duration analysed" field in Annex IV should be optional due to challenges in determining availability impact metrics. These adjustments align standards with practical risk management needs while supporting effective cybersecurity measures.
    Alignment with NIS2 Risk Assessment

17. How could the reporting template for the entity level in Annex IV be adjusted, so that it is easier to fill in based on the Risk Assessment performed for national cybersecurity legislations (such as NIS and NIS2)?

    The use of word "threat" should be changed to "attack vector" as the Annex III does not describe threats but Attack vectors.

18. Do you have any other comments on the Risk Assessment Methodologies?

    In Annex V, to enhance coherence between parties (regions or entities) in reporting and to enable a more efficient analysis at the Union level, a guidance list of minimum recommended processes could be provided