# WindEurope Response to ENTSO-E Public Consultation on Cyber-attack Classification Scale Methodology for the Network Code on Cybersecurity (NCCS)

**Overview**

Under Article 37(8) 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 methodology for the cyber-attack classification scale.
The document will help high-impact and critical-impact entities to assess whether a cyber-attack is reportable according to the NCCS by understanding the gravity level of a cyber-attack. The gravity of a cyber-attack is based on the potential impact and the severity of the cyber-attack. The potential impact is determined by the types of assets affected. The severity of the cyber-attack is estimated according to the position of an attacker in the attack chain.

When high-impact and critical-impact entities assess the gravity of the cyber-attack as critical or high, they must share relevant information with their CSIRTs and competent authorities no later than four hours after assessing that the cyber-attack is reportable.

**Questions**

**Completeness**

1. Title 2 describes the methodology for determining if a cyber-attack is reportable under the NCCS. Is this methodology clear and understandable?

No

The classification of a cyber-attack severity based on Attack-kill chain assessment by using MITRE attack is not advisable. The MITRE attack methodology is developed to describe attacker techniques. As the attacker techniques are not know during the detection, remediation and restoration of a cyber-attack the MITRE framework has little to no applicability in these phases – it may however be used in forensic operations which must be expected to take as long as years. As result the classification of a ongoing or just ended attack by using MITRE is not advisable. Some more guidance needed when an attack is malicious

**Generic**

2. Do you consider that your internal CSIRT will understand the Cyber-attack Classification Scale Methodology for operational use?

   Yes.

   **Comment:**

   The classification of attacks based on the systems attacked is inherently complex, for those who operate a SOC ,as similar systems may exist in different areas and have varying impacts. Consequently, using system types to determine impact can be misleading. - The Perdue model seems more applicable to this use case, at it describes the reach of an attack. And will guide development of detection capabilities and stress the relevance of segmentation which is the most effective security practice. o Physical damage requires access to lower perdue levels 0-2, and these networks are commonly deterministic any unknown activity in these networks may be treated as a suspicious activity that is easily detectable and reportable. As result these activities if confirmed to be unknown may easily be classified as ‘critical’ attacks o Unknown activity in perdue level 3 (PLC/SCADA) networks are also a indication of malicious activity that requires investigation and may be assumed to be ’high’ severity attacks if confirmed. and The general idea of separating impact from severity is very complex, and hard to comprehend.

3. During a crisis, do you think that your operational team, under pressure, will be able to use the Cyber-attack Classification Scale Methodology without any issue?

   No

   We do not operate a CSIRT but a SOC. The use of the classification scheme based on the systems attacked is very complex as similar systems may reside in various areas with various impacts. Therefor the use of system types to determine impact is misguiding. - The Perdue model seems more applicable to this use case, at it describes the reach of an attack. And will guide development of detection capabilities and stress the relevance of segmentation which is the most effective security practice. o Physical damage requires access to lower perdue levels 0-2, and these networks are commonly deterministic any unknown activity in these networks may be treated as a suspicious activity that is easily detectable and reportable. As result these activities if confirmed to be unknown may easily be classified as ‘critical’ attacks o Unknown activity in perdue level 3 (PLC/SCADA) networks are also a indication of malicious activity that requires investigation and may be assumed to be ’high’ severity attacks if confirmed. and The general idea of separating impact from severity is very

complex, and hard to comprehend. Readiness also to be confirmed by an assessment.

**Estimation of the root cause**

4. Article 4 describes the estimation of the root cause. Is the approach to estimate the root cause clear and understandable?

   Yes

   Comment: The requirement to report all incidents unless they are clearly 'not malicious' introduces a challenge, as determining non-malicious activity requires a certain level of effort and clarification. As a result, this approach may lead to a high volume of false positives being reported. Additionally, assessors may require clearer guidance to make accurate and consistent classifications, reducing unnecessary escalations while ensuring that real threats are appropriately addressed.

**Determination of the potential impact of the cyber-attack**

5. Article 5 describes the determination of the potential impact of the cyber attack. Is the approach to determine the potential impact clear and understandable?

   No

   The chain of references back to the 1366/2024 sets the understanding that only corroborate impacts can defined weather an asset is high and critical impacting assets. As result only off-shore wind-parks that connect multiple countries can be such an asset. As result this article not applicable for wind farms, given the reference back to the cross border impact they can only apply to TSO-controlled assets. All wind assets must be assessed to be 'low impact' assets.

**Estimation of the severity of the cyber-attack**

6. Article 6 describes the estimation of the severity of the cyber-attack. Is the approach to estimate the severity clear and understandable?

   No

   The MITRE attack framework has little to no applicability in classification of attacks as it would require a setup where classification is based on a layered defence model. classification of a ongoing or just ended attack by using MITRE is not advisable. Whereas the overdue model is applicable for this.

**Cyber- attack gravity classification**

7. Article 7 describes the approach to determine the gravity of a cyber-attack. Is the approach to determine the gravity clear?

   Yes

   Comment: The general idea of separating impact from severity and combining it with gravity is very complex. As the task is merely to assess the thresholds for reporting the perdue model seems more applicable, as it would allow for detective measures to be applied and balanced.

**Process diagram and matrix**

8. Annex I contains the diagram of the classification process and the gravity matrix. Are the diagrams clear and understandable?

   Yes

9. Annex I contains the diagram of the classification process and the gravity matrix. Are the diagrams at the right level of detail?

   Yes

**Other**

10. Do you have any other comments on the Cyber-attack Classification Scale Methodology?

A threat centric risk assessment based on frameworks like MITRE attack makes good sense. While classification of incidents does not. Given following: 1. Limited knowledge at the time of reporting 2. The MITRE kill chain analysis is applicable for preventive measures as it aims on breaking the chain or guide detective measures. 3. Reporting requirements should be based on the value of the information to the recipient – the classification scheme only confuse.