WindEurope's response to the consultation of the draft network code of sector – specific rules for cybersecurity aspects of cross-border electricity flows

. We welcome the opportunity to comment on the draft network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows.

- Our primary concern with the current draft is that it is very weak in driving harmonisation across the EU regarding the cyber security risk assessment methodology to be applied at national level:
    - In Article 17, the list of participants in the process seems too restrictive, given the scope of impact on the entire electricity value chain. A much broader list of stakeholders in the value chain will have obligations to apply the risk assessment methodology and mitigate cyber security risks. This code will majorly impact the design of generation assets and equipment. Generation asset owners, equipment OEMs and O&M service providers shall be engaged in developing the proposal for the risk assessment methodology together with TSOs, DSOs and ENISA and not only be consulted on this.
    - Based on the proposed Article 28, cyber risk mitigation towards critical infrastructure would have differing national security implications for each member state. There is a high probability that giving each member state a choice of putting a national cyber verification scheme will result in multiple and usually conflicting minimum and advanced cyber security controls across the EU. The net effect would defeat the harmonising purpose of the NCCS. However, if the requirement was to undergo a third-party audit, each member state could retain their national security interests following an EU-wide agreed cyber risk mitigation framework, and the NCCS would not have the impact of driving a multiplicity of cyber security frameworks.
    - Regarding Article 33 (Mapping matrix for electricity cybersecurity controls against standards): while such a matrix would be exceedingly helpful as a reference tool, this would reinforce a cyber-control-centric view of risk mitigation and could potentially enforce conflicting and overlapping controls for compliance among member states.

      For example, if one of the control frameworks satisfies a particular EU member state interpretation of a specific control, does that automatically meet both EU-NIS2 requirements and the NCCS? Or would a TSO have to go through multiple certification or audit schemes for each framework referenced in the matrix? How that will play out is not clear in the Article.

      Instead of a mapping matrix for electricity cybersecurity controls, the unifying effect can be better achieved with a mapping matrix of threat intelligence and vulnerabilities, such as the MITRE ATT&CK™ framework (https://attack.mitre.org/), which will be a very useful tool for harmonization purposes. Such a document could be developed at EU level by the same stakeholder group developing the proposal for the risk assessment methodology which in our view needs to also engage generation asset owners, equipment OEMs and O&M service providers.

We also request first-hand knowledge on attack pathways, vulnerabilities, and useful threat Intelligence regarding advanced persistent threats (APT) attacks that are specific to the energy sector. This needs to be organised and distributed among our community.

- The lack of detailed guidance in the proposed draft risks making the NCCS largely redundant to current European and national legislation such as the NIS2 Directive and the Cyber Resilience Act. The proposed NCCS is insufficiently differentiated from these ongoing legislative projects. This lack of sufficient differentiation might lead to double regulation and bureaucratic overburdening with significant additional costs for asset owners, operators and technology suppliers. If the NCCS is foreseen to override this legislation, this needs to be made clear in the text to avoid misinterpretation at a national level and multiplication of reporting obligations.
- Acceptance of existing national incident reporting systems and established cybersecurity frameworks based on international standards: Some members of the Union already have suitable incident reporting systems in place. These systems for incident reporting should be allowed and supported/fostered to be used without much further adaption.
- The current text brings uncertainty regarding the attribution of liabilities at a national level. For instance, in the case of multinational entities with different member state units, there might be significant variation among member states regarding which entity of the holding will be liable for risk assessment obligations or, for instance, if the network code obligations will fall on the owner or the operator or the technology supplier.