eurelectric
powering people

Network Code on Cybersecurity aspects of cross-border electricity flows

A Eurelectric response paper

November 2023

Eurelectric represents the interests of the electricity industry in Europe. Our work covers all major issues affecting our sector. Our members represent the electricity industry in over 30 European countries.

We cover the entire industry from electricity generation and markets to distribution networks and customer issues. We also have affiliates active on several other continents and business associates from a wide variety of sectors with a direct interest in the electricity industry.

We stand for

The vision of the European power sector is to enable and sustain:
- A vibrant competitive European economy, reliably powered by clean, carbon-neutral energy
- A smart, energy efficient and truly sustainable society for all citizens of Europe

We are committed to lead a cost-effective energy transition by:

investing in clean power generation and transition-enabling solutions, to reduce emissions and actively pursue efforts to become carbon-neutral well before mid-century, taking into account different starting points and commercial availability of key transition technologies;

transforming the energy system to make it more responsive, resilient and efficient. This includes increased use of renewable energy, digitalisation, demand side response and reinforcement of grids so they can function as platforms and enablers for customers, cities and communities;

accelerating the energy transition in other economic sectors by offering competitive electricity as a transformation tool for transport, heating and industry;

embedding sustainability in all parts of our value chain and take measures to support the transformation of existing assets towards a zero carbon society;

innovating to discover the cutting-edge business models and develop the breakthrough technologies that are indispensable to allow our industry to lead this transition.

Dépôt légal: D/2023/12.105/46

WG Technology
WG Thermal & Nuclear
Secretariat Group Distributed Flexibility and Data management
WG Market Integration & Network Codes
WG Retail Market Design
WG Customers & New Services

Contact:
Jessica GARCIA, Advisor - Distribution & Market Facilitationtit –
jgarcia@eurelectric.org

Summary for consultation

Eurelectric welcomes the ongoing efforts to enhance cybersecurity and appreciates this opportunity to respond to the delegated regulation of the European Commission.

Implementation timescales:

Overall, we find the implementation horizon too long. In its current version, the NCCS could take between 7 to 10 years until it is fully implemented, leaving the European electricity grid more vulnerable to cyber-attacks in the meantime. For instance, in the scenario where all deadlines are met, a critical-impact entity will only be obliged to demonstrate compliance with the common electricity cybersecurity framework 10 years after the entry into force of the NCCS.

- We welcome Article 33 creating a mapping matrix to provide the information of which controls in European and international standards would be equivalent to the controls proposed in Article 27. However, It is unnecessary to wait 36 months for the results and it should be changes to 6 months. In addition, we propose in Article 47 to also create a *provisional* mapping matrix for the *provisional* cybersecurity controls, instead of only a list of European and international standards to provide guidance.

- The timeline incoherence between two interdependent requirements should be rectified. The first requirement is for national entities to create a list of national legislation for cybersecurity purposes. The second requirement is for ENTSO-E and EU DSO to develop a provisional list of European and international standards and controls needed for national legislation. The second requirement has a shorter deadline, even though it is secondary to the first requirement.

Information sharing:

- Article 37(3) states that *"Each critical-impact and high-impact entity shall share relevant information related to a reportable cybersecurity incident with its CSIRT and its competent authority..."*, which stipulates double reporting. Communication between CSIRTs and national authorities should be coordinated, but the reporting at entity level should be concentrated in one common mechanism or reporting platform.

- Article 37(8) also stipulates that the notification of a significant incident within the scope of NIS2 Directive "*shall constitute reporting of information under paragraph 3 of this Article*.", which contributes to the argument that the existing reporting lines should be considered and avoid duplication in the reporting process.

- The references to the NIS2 Directive are problematic since the directive has not been implemented yet in the member states which could cause several overlaps. Therefore, NC CS should stress national competent authorities and CSIRTS to streamline the regulatory frameworks. Additionally, To manage control, and comply with new cybersecurity requirements, coordination must take place between both the EU and the national authorities by requirements such as the upcoming NIS-2 and CER Directives, as well as this new regulatory framework. We fear double regulation and more bureaucracy.

Cybersecurity risk assessment methodologies:

- In Article 17(2) there is an obligation to include threat scenarios linked to attacks on the supply chain in the risk methodology at Union level. Perhaps other type of threat, potentially more serious, should also be highlighted.

- There are no references to international standards in the area of risk management (e.g. ISO 27005, ISO 31000, NIST CSF, ENISA requirements). It would be useful to make it clear which guidelines, in terms of established good practices, you have based your risk management proposals on.

Scope:

- There is an incoherence between the Article 31(2) and 25(3.a) and the referral to “other processes” is quite generic and should be eliminated. Entities should clearly understand what the minimum scope of their cybersecurity management system shall include and references to other articles should be limited. Moreover, the scope depends on further work determining the thresholds.

Consultation response

Eurelectric welcomes the ongoing efforts to enhance cybersecurity and appreciates this opportunity to respond to the delegated regulation of the European Commission.

Implementation timescales:

- For all entities in scope of the network code it would be very useful to know which controls in European and international standards would be equivalent to the controls proposed in article 27. We therefore welcome article 33 that creates a mapping matrix to provide this information. However, it comes only within 36 months after the notification of the high- and critical-impact entities. It is unnecessary to wait three years for the results of an exercise that could be completed in 6 months. Therefore, we would propose two changes: in article 33 we would propose to bring the 36 months to create the mapping matrix back to 6 months. In addition, to help entities even more, we would propose in article 47 to also create a provisional mapping matrix for the provisional cybersecurity controls, instead of only a list of European and international standards to provide guidance.

- There is a timeline incoherence regarding two interdependent requirements: the requirement imposed upon the national entities to develop a list of relevant national legislation for the purposes of cybersecurity aspects of cross-border electricity flows, and the subsidiary requirement imposed upon ENTSO-E and EU DSO entity to develop a provisional list of European and International standards and controls required by national legislation. The latter is secondary to the former and yet, it has a shorter deadline. Once designated, the competent national entities are given 6 months to produce the list of relevant legislation, which means 9 months after the Regulation has entered into force. However, the second requirement according is expected to be fulfilled 6 months after the Regulation has entered into force, which amounts to an incoherence.

Scope:

- There is an incoherence between the Article 31(2) and 25(3.a) and the referral to “other processes” is quite generic and should be eliminated. Entities should clearly understand what the minimum scope of their cybersecurity management system shall include and references to other articles should be limited.

- It would be more appropriate to explain the definitions properly instead of giving references to a lot of different articles. Moreover, the scope depends on further work determining the thresholds.

Information sharing:

- According Article 37(5), entities are not obliged to report unpatched actively exploited vulnerabilities, which, by definition, already constitute cyber-attacks. We not only disagree with this voluntary/non-mandatory requirement, but even with this reactive approach. Cybersecurity demands a more proactive approach, and therefore we suggest that any unpatched 0-day vulnerability must be immediately reported, even before being exploited, to ensure they are timely addressed, avoiding exploitation of said vulnerabilities and the consequent occurrence of cyber-attacks.

- Article 37(3) states that *“Each critical-impact and high-impact entity shall share relevant information related to a reportable cybersecurity incident with its CSIRT and its competent authority...”*, which stipulates double reporting. Communication between CSIRTs and national authorities should be coordinated and stipulated within the proposed network

code, but the reporting at entity level should be concentrated in one common mechanism or reporting platform.

- To manage control, and comply with new cybersecurity requirements, coordination must take place between both the EU and the national authorities by requirements such as the upcoming NIS-2 and CER Directives, as well as this new regulatory framework. Article 37(8) also stipulates that the notification of a significant incident within the scope of NIS2 Directive "*shall constitute reporting of information under paragraph 3 of this Article*.", which contributes to the argument that the existing reporting lines should be taken into account and avoid duplication in the reporting process. In the regulations, it is stated that "the general rules on the security of network and information systems laid down in Directive (EU) 2022/255511 (NIS2 Directive) are complemented by the network code." NIS2 has not been implemented yet in the EU member states. This may lead to several overlaps, and this should be considered in the implementations. Therefore, NCCS should stress national competent authorities and CSIRTs to streamline the regulatory frameworks.

- A final remark regarding both of these articles is the incoherence between the reporting deadlines – it is unclear how the reporting of an entity under NIS2 Directive can constitute a reporting of information under Article 37(3), if Article 23 (4.a) of the NIS2 Directive stipulates a 24-hour initial report deadline whereas Article 37(3) of the NCCS stipulates a 4-hour initial report deadline. If the NCCS intends to be more demanding than the NIS2 Directive, due to the criticality of the electricity sector, Article 37(8) should include the caveat of the NCCS more demanding deadline.

- Eurelectric also suggests to provide guidance on Information Sharing procedures regarding Cyber Threats (what kind of information about Cyber Threats, when is mandatory notify, how to notify, etc.).

Cybersecurity risk assessment methodologies:

- In Article 17(2) there is an obligation to include threat scenarios linked to attacks on the supply chain in the risk methodology at Union level. Perhaps other type of threat, potentially more serious, should also be highlighted.

- There are no references to international standards in the area of risk management (e.g. ISO 27005, ISO 31000, NIST CSF, ENISA requirements). It would be useful to make it clear which guidelines, in terms of established good practices, you have based your risk management proposals on.

- It is not very clear what the roles and responsibilities of the different entities involved in the risk assessment were, including the operators, the entities involved in the risk assessment and the entities involved in the risk assessment.

- Article 17 is very important and the development and implementation of a methodology for risk assessment. Defining the Electricity Cybersecurity Risk Index (ECRI) for high-impact and critical-impact thresholds is crucial. As well as defining a list of Union-wide high-impact and critical-impact processes. We are concerned about the fulfillment of requirements of timelines here, as this work must have a top priority in order not to place uncertain demands on the entities.

- A method for cybersecurity risk assessments must be developed based on clear input values and risk analysis scenarios to promote an appropriate level of analysis. The demand

for increased resilience has shifted to a risk-based approach that allows resilience to be adjusted based on the actual risk profile. Different devices face different threats, requiring tailored levels of protection to prevent either over- or under-protection of critical systems. Therefore, we see advantages in this adaptability to consider methodologies at different levels depending on the degree of impact of cross-border electricity flows.

- At the current version, the Network Code is not fully harmonized with the framework of EU and national regulations in the field of Cyber Risk management on the electricity sector. To provide some concrete examples, there are Network Code measures for entities, such as (i) those related to the implementation of the Cyber Risk Management program (art. 33), (ii) of minimum and advanced measures (art. 28), (iii) of measures on the supply chain (art. 32) and (iv) the development of a cybersecurity management system (art. 31) which significantly overlap with EU (NIS 2.0 in particular) and National Regulations. The risk is to generate different approaches to mitigate similar Cyber Risks by creating an overload of compliance to manage for involved entities, primarily DSO and TSO.

Recovery of costs:

- We welcome the recognition that the costs incurred by DSOs which stem from the obligations in the NCCS should be fully recovered through network tariffs or other appropriate mechanisms.

Common Approach:

- In Recital 18, as neighbour countries evolve at different rates in the use of cybersecurity risks assessment systems, a mention to the Benchmarking (Article 13) should appear here, setting a reference for comparison and systems evolvement over time.

Monitoring:

- Recital 23 is missing the reference to forensic analysis that can improve the preparedness of other grid operators regarding same context awareness.

Cooperation between relevant authorities and bodies at national level:

- Concerning Article 5, Public and private R&D entities, with expertise in (cyber)security subject, should be invited to participate as observers, helping in debriefing sessions and further getting insights for their research and innovation work/activities.

Specific comments

Legal elements of the delegated act

In the regulations, it is stated that “the general rules on the security of network and information systems laid down in Directive (EU) 2022/255511 (NIS2 Directive) are complemented by the network code.” NIS2 has not been implemented yet in the EU. Therefore, it is hard to follow and verify the referrals to NIS2. Furthermore, in many countries, the process of national implementation is ongoing and may present stricter implementations than in the Directive. This may lead to several overlaps, and this should be considered in the implementations. Therefore, NC CS should stress national competent authorities and CSIRTS to streamline the regulatory frameworks. Due to redundancy and insufficient differentiation from ongoing legislative projects, e.g. the NIS2 Directive implementation, there is also a considerable risk of double regulation and consequently, bureaucratic overburdening.

The cycle for updating NIS2 and CER Directive is 4 years, therefore this time horizon preferably be used in NCCS.

Article 38 Detection of cybersecurity incidents and handling of related information

Multinational electricity grid entities should not have to report to several national authorities, and CSIRTs, to avoid duplications of obligations as the proposal overlaps with several existing regulations.

As cyber threats became more sophisticated and widespread multinational distribution system operators (DSOs) faced a significant challenge. It is extremely important to ensure methodology, but above all the feasibility of reporting as well as follow-up and reporting back to the entities that report incidents. More questions from the authorities do not always mean that the businesses get a better picture of the situation. The new proposal must be manageable for large entities as well as small energy entities. The requirements for reporting will require increased resources within entities, therefore the reporting requirement as well as the costs must be set at a reasonable level.

The incident reporting process must therefore be clearer and identify gaps according to the regulation related to the NIS2 Directive. A single, unified reporting process would be more efficient to avoid delays or incomplete reporting and avoid duplications of obligations. However, collecting information about incidents at an EU body can also involve risks of hacker attacks and leaking knowledge about weaknesses in national systems.

Conclusion

The regulation of a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows provides a game shift. Transmission (TSO) and distribution system operators DSO) as well as authorities need to act quickly to achieve compliance with the comprehensive framework as well as increase protection of the energy infrastructure from cyber threats, including the increasing threat of AI attacks. Knowledge of production facilities and the function of other electricity market participants is also important to consider in the development of methodology.

The question of how the energy industry protects its distributions against cyberattacks is a highly topical issue, and interruptions in electricity supply that depend on cyber security mean the risk of large costs for society. It is therefore extremely important that both national handling of the regulation is accurate and cost-effective and provide the opportunity for national adaptations in risk management if necessary.

Eurelectric pursues in all its activities the application of the following sustainable development values:

Economic Development

- Growth, added-value, efficiency

Environmental Leadership

- Commitment, innovation, pro-activeness

Social Responsibility

- Transparency, ethics, accountability

Union of the Electricity Industry - Eurelectric aisbl
Boulevard de l'Impératrice, 66 – bte 2 - 1000 Brussels, Belgium
Tel: + 32 2 515 10 00 - VAT: BE 0462 679 112 • www.eurelectric.org
EU Transparency Register number: 4271427696-87